The **Value** Builder System™

The Value Builder System™ Compliance Package

Section One: Company Information

The Value Builder System™ (operating name) and Built to Sell, Inc. (legal name), is a corporation started in 2012 by John Warrillow. The company is privately owned and located in Toronto, Ontario, Canada.

More information on The Value Builder System can be found at http://valuebuilder.com.

Description of Business:

The Value Builder System offers a suite of tools and services designed to help business owners increase the value of their companies. The Value Builder Report evaluates businesses based on eight key drivers of value, providing actionable insights for improving a company's worth to potential buyers. The system supports business owners through a network of trained advisors and is aimed at optimizing business value in preparation for a successful exit or sale.

The core features and services of The Value Builder System include:

1. Assess: Our three owner-friendly assessments offer a 360-degree view of a company's value and the owner's personal and financial readiness to exit their business
2. Grow: Resources and strategies to help owner grow the value of their business
3. Nurture: Our nurturing system features owner-friendly content that is pre-tested and optimized using our proprietary panel of more than 25,000 business owners

Section Two: Technology and Development

Our system is designed as a micro services architecture and as such is very scalable. As a processor of privileged confidential information, compliance with

international data privacy law is essential to our design and management process.

Web / Mobile Availability:

The Value Builder System™ is available on a 99.9% uptime basis. We have a customer base that is global and therefore we 24/7 real-time monitor our uptime across multiple locations and devices. We use tools such as New Relic, PagerDuty and Google Analytics. Our aim is to have <2.5 second page load time.

Development Lifecycle:

Our team uses an Agile SDLC. Updates are provided on a biweekly basis with major releases on a quarterly basis. Urgent fixes are done on an as needed basis.

Features are built with a two-week sprint cycle. Each feature must pass rigorous automated Quality Assurance testing and functional acceptance testing framework before being accepted as done. Release candidates go through full regression testing (automated and manual) before being approved and then being released.

We are currently delivering against a 12-month roadmap for major features that involves business case and ideation. Typically, larger features are iteratively developed to a viable product over multiple two-week sprints and released as part of a major release on a quarterly basis. Smaller improvements and bug fixes are done iteratively with minor releases every 2 weeks.

Test System:

Our testing and production system are hosted via AWS in North America. Our testing has multiple region variations including European specific issues (i.e., GDPR), Australian and North American issues. All features are tested via a mixture of human testers and automated tests looking for functional issues, bugs and security.

System Maintenance and Support:

Our system has a 24/7 on-call team to manage any outages or issues. Issues are prioritized and triaged with fixes carried out immediately or added to our roadmap depending on severity and impact. Currently system maintenance and releases are carried out at scheduled low usage windows (i.e. 3am EST).

Integration:

There is no integration required by our system. Typically our customers integrate outgoing marketing and transactional email communications from our system to go through customers Google Apps, Office 365 accounts or custom STMP environments.

Disaster Recovery and Business Continuity:

We have an internal Disaster Recovery and Business Continuity policy with the goal of 18hr recovery time for any worst-case outage excluding unlikely Acts of God. This is above and beyond a half hour response time goal for more likely outages or issues. Our less critical marketing tools and external websites have a recovery goal of 48hrs. Backups of Customer Data and Application is done nightly with daily backups stored for a week, weekly for a month and monthly for a year. Managed risks with appropriate response include but are not limited to, system or physical failure, physical disasters, data corruption, provider availability, deployment failures as well employee continuity.

Section Three: Data Security and Privacy

Client Identifiable Data and Privacy:

Usage of our private information is laid out in our privacy policy this includes obligations to relevant privacy laws, responsibilities for data, breach reporting requirements and the right to be forgotten.

We collect name, email address, business name, and business address. Built to Sell also collects business information, which may be entered or obtained and associated with personally identifiable information, such as, but not limited to, the business´s revenue and profitability. There are also questions about age (not DOB) as well other information that could be used to identify the user.

Handling and Storing of Sensitive Data:

The Value Builder System™ makes a concerted effort to restrict access to personally identifiable information to those employees and service providers who have a need to know that information and to maintain physical, electronic, and procedural safeguards to guard personally identifiable information. We use third party providers to store and host our data. Data is encrypted at rest on a drive basis. This data and its backups are access controlled with industry standard security. Our hosting provider, AWS, is Compliant with most data security standards including HIPPA and SOC 2.

The **Value** Builder System™

If data is required to analyze or improve our system, we would use an aggregate with non-identifying information or anonymized copy.

Data Exchange:

Currently you can access our stored information in the following ways:

- Reports are sent to contacts via email
- Advisors can access assessment reports and download via browser
- Contact information and preferences can be viewed at a user, advisor, team and company level via a browser
- For advisors that use our Value Builder Engagement tool, the business owner and advisor can access business analysis tools via their browser.

We can export any data as a special request to our Customer Success team. This would be only given to designated company administrators via a secure transfer method.

Currently our Support team and Product team are the only people able to access production data. Our team and any sub-contractors pass background checks, training and have policies governing appropriate use of customer data.

Data Usage:

- Data may be used to analyze and improve our algorithms for generating reports and our score. Contacts assessment answers are used in the aggregate without personally identifiable information
- Our team may access information to troubleshoot issues upon permission from a customer
- Our team may use an anonymized copy of data for testing of improvements.

Security Features Summary:

- Role based access with password policies and user identity verification
    - All users are required to have two factor authentication to sign into our system
- Protection of data at rest on physical drives (i.e., encryption)
- SSL encryption of data transferred (i.e., web browser)
- Secure communication protocols and DMZ layer for our application-level communications.

- Application Servers are locked down to common ports for external access or specific IPs for development level access (ie office IP's) with no direct access to user data
- Security reviews of hosting environment setup are done on a regular basis as well as application-level testing and review for security vulnerabilities (i.e. SQL injection and permissions) are included in the Software Development Lifecycle for new features.

Asset Management

- Computer and any data mediums are controlled and tracked with administrative control
- Company Shared Drive folder has role-based control, data access is tracked (Onedrive)
- Customer data is accessed through shared company applications with role-based access and access tracking.
- All passwords our encrypted with company LastPass (two factor authentication) and local passwords are not allowed as per policy
- After termination, there is a SOP for office manager to lock out users from applications and recover assets
- All hard drives with data should be destroyed on discontinuation.

Physical Security

- AWS data is stored in Soc 2 compliant facilities
- No data is stored on premise
- Employee Computers with access are encrypted and protected by two factor passwords. Strict Role Based Access with password control programs used. (i.e. LastPass).

Development Lifecycle

- During Development Code review must ask question, "does this protect against SQL injection, is there any possible known vulnerabilities that this may harm"
- QA acceptance testing should consider basic security testing including SQL injection and permissions
- Privacy by design and testing as release criteria for new features

Backups

- Are done via our DR Policy (every day for a week, one week for a month, monthly for a year)
- Snapshot of entire AWS Instance only accessible by AWS admins

- Only AWS Release Engineer has access to backups along with Director of Product and Director of Operations
- AWS use two factor authentication or secure key (3 individuals with ownership) for direct server access
- Stored in encrypted state
- Please see DR Policy for more info

Breach or Privacy Request

- All Outages, Suspected intrusion and Response go through our SOP process
    - Triage of state of issue (ongoing or in the past)
    - Act to shutdown any active breach
    - Investigate impact of breach and discuss internal response
    - Notify any affected customers as our Privacy Policy
    - Investigate GDPR obligations to notify regulator
- Right to be Forgotten requests are handled as per normal SLDC lifecycle process

Intrusion Scanning

- Yearly scan with all high and medium priority items fixed
- Bi-annual review by third party Dev Operations Contractor for system configuration issues

Vendor/Subcontractors and Human Resources

- Privacy and Security are a requirement in selection process with Agreements about access to and ownership of scoped data
- Breech and Data Security processes in place for any vendor that deals with private information
- Sub-contractors and Built to Sell Inc employees have policies and contractual clauses governing data security, ownership and privacy. We reserve the right for background checks for customer facing and customer data access
- Employees have asset management program governing security and setup of company devices, access restrictions and termination procedures.
- Sub Contractors are governed by Data Processing Agreements before accessing PI data
- There is access control and password management software employed for continuity and security

Cyber Insurance

- The company maintains Cyber Insurance to cover any liabilities related to delivering this policy

Soc 2 or SAE Compliance

- We make no claim to compliance with these standards. However, our hosting facilities are compliant. (AWS).

Uptime Exceptions

- Exceptions: No period of Service degradation or inoperability will be included in calculating availability to the extent that such downtime or degradation is due to any of the following:
    - Client's misuse of the Services.
    - Internet or other network traffic problems other than problems arising in or from networks actually or required to be provided or controlled by Supplier.
    - Client's failure to meet any minimum hardware or software requirements set forth in the Specifications; or
    - Scheduled Downtime
    - Scheduled Downtime is generally between 2am and 6am EST on Tuesdays or Thursdays. Anything longer than an hour would be separately scheduled to a low usage time with notifications.