VSM

Vendor Security Measurement

BuiltWith® Pty Ltd
35th Floor One International Towers
100 Barangaroo Avenue
Sydney NSW 2000
Australia

Created:
January 2016

Last Revised:
March 2023

Security Measures

Access Control

- Unauthorized persons are prevented from gaining physical access to premises, buildings or rooms, where data processing systems are located which process personal data
- Controls implemented to specify authorized individuals permitted to access personal data
- Implemented an access control process to avoid unauthorized access to Customer's premises
- Implemented an access control process to restrict access to data centres / rooms where data servers are located
- Utilized video surveillance and alarm devices with reference to access areas
- Ensured that personnel without access authorization (e.g. technicians, cleaning personnel) are accompanied all times when access data processing areas

System Access Control

- Processing systems are prevented from being used without authorization
- All systems processing personal data (this includes remote access) are password protected and firewalled and 2FA.

- Dedicated user IDs for authentication against systems user management for every individual
- Assigned individual user passwords for authentication
- Access control is supported by an authentication system
- Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function
- Implemented a password policy that prohibits the sharing of passwords, outlines processes after a disclosure of a password and requires the regular change of passwords
- Ensured that passwords are always stored in encrypted form
- Implemented a proper procedure to deactivate user account, when a user leaves the company or function
- Implemented a proper process to adjust administrator permissions, when an administrator leaves company or function
- Implemented a process to log all access to systems and review those logs for security incidents

Data Access Control

- Persons entitled to use a data processing system shall gain access only to the data to which they have a right of access, and personal data must not be read, copied, modified or removed without authorization in the course of processing
- Restricted access to files and programs based on a "need-to-know-basis"
- Stored physical media containing personal data in secured areas
- Controls to prevent use/installation of unauthorized hardware and/or software
- Established rules for the safe and permanent destruction of data that are no longer required
- Controls to grant access only to authorized personnel and to assign only the minimum permissions necessary for those personal to access personal data in the performance of their function

Data Transmission Control

- Personal data cannot be read, copied, modified or removed without authorization during transfer or storage and it shall be possible to establish to whom personal data was transferred
- Encrypt data during any transmission

Data Entry Control

- Retrospectively be able to examine and establish whether and by whom personal data have been entered into data processing systems, modified or removed.
- Controls to log administrators' and users' activities
- Controls to permit only authorized personnel to modify any personal data within the scope of their function

Job Control

- Personal data being processed in the performance of a service for the Company shall be processed solely in accordance with the services agreement in place between the Company and the Vendor and in accordance with the instructions of the Company
- Established controls to ensure processing of personal data only for contractual performance
- Controls to ensure staff members and contractors comply with written instructions or contracts

- Ensured that data is always physically or logically separated so that, in each step of the processing, the client from whom personal data originates can be identified.

Availability Control

- Personal data shall be protected against disclosure, accidental or unauthorized destruction or loss.
- Arrangements to create back-up copies stored in specially protected environments
- Arrangements to perform regular restore tests from those backups
- Contingency plans or business recovery strategies
- Controls to ensure that personal data is not used for any purpose other than for the purposes it has been contracted to perform
- Controls to prevent removal of personal data from Vendor's business computers or premises for any reason (unless Customer has specifically authorized such removal for business purposes).
- Controls to use only authorized business equipment to perform the services
- Controls to ensure that whenever a staff member leaves its desk unattended during the day and prior to leaving the office at the end of the day, he/she places materials containing personal data in a safe and secure environment such as a locked desk drawer, filing cabinet, or other secured storage space. (clean desk)
- Implemented a process for secure disposal of documents or data carriers containing personal data
- Implemented network firewalls to prevent unauthorized access to systems and services
- Ensured that each system used to process personal data runs an up to date antivirus solution

Organizational Requirements

- The internal organization of the Vendor shall meet the specific requirements of data protection
- Designated a data protection officer (or a responsible person if a data protection officer is not required by law)
- Obtained the written commitment of the employees to maintain confidentiality
- Trained staff on data privacy and data security
- Implemented a formal security incident response process that is consistently followed for the management of security incidents
- Trained staff in the security incident responder roles on the security incident process

Sub Processors

Our sharing of your personal data is very limited and a requirement for us to operate BuiltWith. All third parties are listed below.

The email addresses that provide consent will be processed by 3rd party email delivery service provider Postmark. See their privacy page here - https://postmarkapp.com/eu-privacy

If you sign up for payment with credit card and/or PayPal your personal details will be processed by Braintree/PayPal, see their privacy policy here - https://www.paypal.com/en/webapps/mpp/ua/privacy-full

If you sign up for payment with credit card you can optionally enable your account using our "know your customer" automated process provided by Persona, see their privacy policy here - https://withpersona.com/legal/privacy-policy

If you sign up for payments with PayPal or credit card your PII may be stored in our accounting system Xero, see their privacy policy here - https://www.xero.com/au/legal/privacy/

If you sign up for payments with Cryptocurrency through Coinbase your email may be processed by Coinbase, see their privacy policy here - https://www.coinbase.com/legal/privacy?locale=en

If you sign up for payments with Cryptocurrency through CoinPayments your email may be processed by CoinPayments, see their privacy policy here - https://www.coinpayments.net/help-privacy

If you choose to authenticate with Google you data may be processed by Alphabet Inc, see their privacy policy here - https://policies.google.com/privacy

If you choose to authenticate with Amazon you data may be processed by Amazon Inc, see their privacy policy here - https://aws.amazon.com/privacy/

In certain situations, BuiltWith Pty Ltd may be required to disclose personal data in response to lawful requests by public authorities, including to meet security or law enforcement requirements. We may also disclose your personal information as required by law, such as to comply with a subpoena or other legal process, when we believe in good faith that disclosure is necessary to protect our rights, when we believe there is a violation to our terms, protect your safety or the safety of others, investigate fraud, or respond to a government request

Infrastructure

BuiltWith Pty Ltd is PCI DSS as monitored by SecurityMetrics. BuiltWith data centers are ISO/IEC 27001 certified, SOC 1 Type II and SOC 2 Type II certified. Servers that process personal data are HSTS enabled, ensuring end-to-end encryption of your information.

Our short term encrypted backups are stored at Dropbox, ISO 27018 certified data center. See their privacy policy here - https://www.dropbox.com/privacy
Our addtional backups are encrypted backups stored at Backblaze, ISO 27001:2013 SOC-2 certified data center. See their privacy policy here - https://www.backblaze.com/company/privacy.html

Our data center is located in Canada. We have no plans to operate servers within the EU or the United States of America that store personal information.

Infrastructure Layout