SOC2

BuiltWith® Pty Ltd
Level 35 - One International Towers
100 Barangaroo Avenue
Sydney NSW 2000
Australia

DATE: 3rd Nov 2023
SOC2 Self Assesment

SOC 2 Self Assessment	Response
Has your organization identified the key systems required to provide services to clients?	**Yes**
Does your organization have monitoring activities in place to evaluate the effectiveness of your internal security controls?	**Yes** Endpoint config weakness monitoring Firewall change monitoring Anti-Virus/Malware Software monitoring
Has your organization documented control activities to mitigate risks and achieve the organization's objectives?	**Yes**
Has your organization performed a risk assessment?	**Yes** Third Party provider also performs risk assessment
Has your organization identified, selected, and developed mitigation strategies for addressing potential security risks (both for your business and for any associated vendors and partners)?	**Yes** No non-compliant third party data/network provider in use.
Does your organization conduct background verification for all your employees as a process?	No employees have access to any computer system except 2 directors of BuiltWith from 2 secure locations.
Does your organization you have Multi-factor Authentication (MFA) and Password Manager enabled for its employees?	MFA required on all third party services and network devices.
Does your organization conduct a vendor risk assessment, and are those conducted periodically?	Only ISO27001 vendors host BuiltWith systems (requirement).
Does your organization have an Incident Management Policy in place?	**Yes**
Does your organization have a Threat Management System in place?	**Yes** Three level thread prevention firewall Cold store backups.
Does your organization have a formal data retention and disposal policy?	**Yes** No customer uploaded data stored beyond 30 days.
Does your organization have established privacy policies and notices in accordance with applicable requirements?	**Yes**
Does your organization encrypt its production databases at REST?	TDE for all databases. All data transmission via TLS1.1+ HTTPS SSL only.
Does your organization have ransomware/ malware protection installed? And you systems encrypted?	**Yes**
Does you organization monitor and log access to identify anomalies and incidents?	**Yes** 5 minute granularity with alerting.
Does your organization have Mobile Device Management (MDMs) enabled?	No mobile device has access to network outside of 2 physical locations.