

## *Exposcan use the Entegy Core Platform for client data Collection*

At Exposcan Pty Ltd, we are committed to ensuring the protection and confidentiality of personal data in compliance with applicable data protection laws and regulations. Our approach to data compliance is integral to maintaining trust with our customers, employees, and business partners. When you use our products, you can be sure that your information is safe with us.

### **Contact Information**

For any questions, concerns, or requests related to data protection, please contact our Data Protection Officer - Email: [info@exposcan.net.au](mailto:info@exposcan.net.au)

Below is an overview of our security practices within our key operational systems.

### **1. Hosting Environment**

The Exposcan/Entegy's platform is entirely hosted on the Amazon Web Service cloud infrastructure in Sydney region. Amazon provide a secure, stable and almost infinitely scalable platform to ensure we can satisfy the security and bandwidth requirements of our diverse customer base. For further information of the AWS platform and their security policies and measures, please visit: <https://aws.amazon.com/security>

The Exposcan Entegy Core hosts its services on the AWS Platform. We leverage many of their services to provide a resilient service. Database Data is stored within Amazon Relational Database Service (RDS). Our RDS server takes nightly snapshots while also having point-in-time recovery provided by RDS. Assets are stored on Amazon's S3 service. Amazon S3 is designed to have an availability (uptime) of 99.99% and designed to achieve 99.999999999% durability of an object (file) over a given year. Further assets are served using Amazon CloudFront CDN over HTTPS. CloudFront provides over 50 edge locations where files are cached and served from providing low latency fast asset delivery.

CMS Servers run on Amazon Elastic Compute Cloud (EC2), All our servers are stateless, creating no files on them. Runtime data for the servers comes from Amazon Elastic Block Store (EBS). We create EBS Snapshots after major updates so that we can spawn already configured new servers if required.

API is provided by Amazon Elastic Beanstalk. It's setup behind a load balancer to auto scale under load, or in the rare event a EC2 API server stops responding.

### **2. Data Protection Commitment**

We adhere to all relevant data protection laws and regulations, including but not limited to The Australian Privacy Act 1988 (Privacy Act). We are dedicated to ensuring that all personal data collected, stored, processed, and shared by clients of Exposcan is managed securely and responsibly. This includes the collection, use, storage and disclosure of personal information in the federal public sector and in the private sector.

### 3. Exposcan Data Collection and Use of the Entegy Core

We collect only the data necessary for legitimate business purposes, and we ensure that personal data is collected with the knowledge and consent of individuals when required. The data we collect is used solely for the purposes outlined at the time of collection and will not be shared with third parties without proper consent, unless required by law.

All connections to the Exposcan Entegy CMS are sent securely using Industry Standard Encryption, Transport Layer Security (TLS). We score an overall A rating on the Qualys SSL Labs, which is recognised as a leader the in the security community (<https://www.ssllabs.com>).

HSTS are used to force browsers to only use HTTPS when connecting to the Entegy Core. This is combined with server-side redirects to redirect browsers that do not support HSTS to use HTTPS. The ciphers are configured and key exchange so that all modern browsers use Perfect Forward Secrecy, to prevent decoding of captured data in the event of a new zero-day vulnerability like HeartBleed.

### 4. Data Security

We have implemented robust technical and organisational measures to protect personal data from unauthorized access, disclosure, alteration, and destruction. These measures include encryption, access controls, regular audits, and staff training.

### 5. Staff

The Exposcan Entegy Core develops its software in its entirety within Australia. We do not outsource development and always maintain complete control of product development in-house. All developers are employed full time and does not utilise the services of contractors, temporary or overseas developers. All code is backed up securely offsite on AWS.

### 6. Data Retention

We retain personal data only for as long as necessary to fulfill the purposes for which it was collected or to comply with legal requirements. When personal data is no longer needed, it is securely deleted or anonymized.

### 7. Third-Party Vendors

Where applicable, we ensure that third-party vendors and service providers who process personal data on our behalf are compliant with relevant data protection laws and have the necessary security measures in place to protect that data.

Access to our CMS is restricted to authorized users with varying levels of permissions. All passwords are salted and hashed which are unable to be decrypted by Exposcan, Entegy or anyone else. Devices must be registered with the Exposcan API before being able to request or submit data. Security policies around registering can be configured on an app by app basis allowing complete flexibility around who can access content.

### 8. Rights of Data Subjects

We respect the rights of individuals in relation to their personal data. These rights may include the right to access, correct, delete, or restrict the processing of personal data, as well as the right to object to processing and the right to data portability. Individuals can exercise their rights by contacting us using the details provided.

### 9. Monitoring & Server Updates

All data holding services run 24/7 uptime monitoring ensuring swift response in the event of a server incident. We endeavour to apply all critical server security patches as soon as they are available and maintain a regular server software update schedule.

### 10. Data Breach Notification

In the event of a data breach, we will notify the relevant authorities and affected individuals in accordance with applicable laws and regulations. We will take prompt action to investigate and mitigate any potential risks to personal data.

### 11. Compliance and Monitoring

We regularly review and update our data protection practices to ensure compliance with evolving data protection laws. Our data protection officer or designated compliance team oversees our adherence to these practices and ensures that all employees are trained on data protection policies.

#### Privacy Policy

Details of the Exposcan Privacy Policy can be viewed online at:

[ExpoScan Privacy Policy](#)

Details of the Entegy current Privacy Policy can be viewed online at <https://secure.entegy.com.au/Privacy/>

Details of the Entegy Data Compliance Statement can be viewed online

At [Security information for the CMS – Entegy](#)