Data Security

Our Colocator location intelligence software collects, processes and stores data for the provision of location-based services to our clients. This document details the policies and procedures that Crowd Connected has in place in respect of the protection of that data.

Background

- The Colocator application is deployed on Amazon Web Services (AWS) environment, including Amazon Elastic Cloud Computing (EC2), Amazon Simple Storage Solution (S3), Amazon Dynamo DB (Dynamo) and Amazon Kinesis (Kinesis). This cloud computing platform has high availability and reliability, and is used by a wide range of organisations.
- ISO 27001/27002 is a widely-adopted global security standard set by the International Organization for Standards (ISO). Achieving ISO 27001 certification requires the company to demonstrate a systematic and ongoing approach to managing information security risks that affect the confidentiality, integrity, and availability of company and customer information. AWS has achieved ISO 27001 certification of its Information Security Management System (ISMS) covering infrastructure, data centers, and services including Amazon Elastic Compute Cloud (Amazon EC2) and Amazon Simple Storage Service (Amazon S3).
- AWS' ISO 27001 certification includes all its data centres in all regions utilised by Crowd Connected. AWS has established a formal program to maintain the certification.
- AWS manages dozens of other compliance programs in its infrastructure designed such that AWS can attest that control objectives are appropriately designed and that the individual controls defined to safeguard customer data are operating effectively
- For further details on security in the Amazon cloud environment, visit http://aws.amazon.com/security.

Physical Security

(i) Data centres:

- Physical access to AWS data centres is controlled both at the perimeter and at building ingress points by professional security staff utilising video surveillance, intrusion detection systems, and other electronic means.
- All visitors and contractors are required to present identification and are signed in and continually escorted by authorised staff.
- Authorised staff must pass two-factor authentication a minimum of two times to access data centre floors. All physical access to data centres by AWS employees is logged and audited routinely.

(ii) Crowd Connected office premises:

- Physical access is controlled at building ingress points with 24/7 security.
- Crowd Connected's offices require electronic pass-card access and are securely locked when unattended. Access to keys is strictly controlled.
- All visitors and contractors are required to present identification and are signed in and escorted by authorised staff.
- It is company policy that staff secure desktop and laptop computer access via password-protected access. Authorised staff may be granted remote access to office-based computers, but always on a password-protected basis.

Data Security

- Crowd Connected uses Transport Layer Security (TLS) encryption (also known as SSL or HTTPS) for all data transmission over the internet.
- All data in S3, EC2 and Dynamo is encrypted at rest using strong encryption (AES-256-XTS).
- Amazon EC2 provides a complete firewall solution. The mandatory inbound firewall is configured in a "default deny" mode, requiring the Amazon EC2 customer to explicitly open any ports to allow inbound traffic. The traffic may be restricted by protocol, by service port, as well as by source IP address (individual IP or CIDR block).
  Amazon have implemented specific measures against the following threats:
  - Distributed Denial Of Service (DDoS) attacks.
  - Man In the Middle (MITM) attacks.
  - IP spoofing.
  - Port scanning.
  - Packet sniffing by other tenants.
- Backups:
  - S3 data has 99.99% durability, and where required is subject to versioning to enable restoration in the event of deletion.
  - Dynamo database tables have, where required, point in time restore enable.
- Access to data and systems:
  - At the AWS level, AWS Root credentials are limited and always have multi factor authentication enabled. Use of other AWS credentials/keys is limited, monitored, and auditable.
  - Colocator API access is via username / password or API Key Pair. Passwords and secret keys are stored encrypted, and are never exposed in plain text. All API use is logged and auditable at a user level. Minimum password standards

are enforced. Granular permissions are set for each set of credentials, granting the minimum required read / write capability for each individual API.

- SSH access to EC2 servers is generally never needed and access is prevented using AWS level security groups. Access is only enabled when specifically required for testing / debugging, and then is restricted by IP address to Crowd Connected's office. Key only (no password) access is enforced, and logins are non root.

Software Security

- Colocator web console uses Crowd Connected's proprietary APIs which are password protected. API access requires a 12-character minimum for user passwords.
- The Colocator web console has a self-service password reset option.
- Colocator customers may control the individual permissions for individuals accessing under their accounts.
- Crowd Connected provides anti-virus protection software on commonly affected systems vulnerable to virus infections and such software protection is regularly updated in line with best practice and in accordance with advice from applicable anti-virus software suppliers.
- Change control procedures are documented and maintained in relation to the Colocator code base.

Monitoring / logging

- AWS cloudtrail is used to log every AWS API call, so that all usage is auditable.
- All Colocator API activity is logged and monitored, and logs may be used for forensic analysis.

Employees

- Crowd Connected has implemented an appropriate pre-employment screening policy.
- Employees are trained in the appropriate handling of data and security awareness, appropriate to their individual role/responsibilities.
- Crowd Connected's policy is to limit employee access to systems/data consistent with their individual role/responsibilities. Access to customer information and other data is therefore on an 'as required basis' for support reasons.

Incident response protocols

- Data security is the responsibility of Crowd Connected's directors.
- Need to report an incident? Have a question, concern, or comment about Crowd Connected's data security? Please contact datasecurity@crowdconnected.com. Crowd Connected will conduct a thorough review of the incident and provide the findings to the user that requested the review.

v2.0, updated May 2018