CROWCON
Detecting Gas Saving Lives

Crowcon Data solution

IT Security FAQ’s

03/12/2019

Security Policy & Assurance Reports

Q; Do you have a Security Policy in place that is aligned with international industry standards? e.g. ISO 27001:2013.

A; Crowcon's data solution is standalone and does not interact with any incumbent systems.

Crowcon is GDPR compliant and has all necessary personnel, policies and processes in place, In line with this, Crowcon's security covers the following areas;

Technical security;

Crowcon are a wholly owned Halma company (FTSE100 company). Crowcon's data solution is hosted on the Halma MS Azure instance and thus conform to their IT policies.

As such; annual independent penetration testing is conducted with all critical, high and medium risks remediated.

Monthly vulnerability scans are performed against all systems (& associated with the) solution with all issues resolved. We have a minimum monthly patching process for all elements of the service to ensure security patches are applied to, for example, servers and network infrastructure.

The customer welcome to perform their own testing - we ask that you inform Crowcon and Halma that you are completing this testing.

In addition Crowcon have an active DR and backup policy.

Operational Security;

Crowcon adhere to Halma Group policies covering; acceptable use, data handling (GDPR), password management and DR.

Security SPOC

Q; Do you have a single point of contact for security related questions, issues and incidents? Please explain how you can meet this requirement & describe the process.

A; Crowcon have a support procedure with contact names and escalation points, in line with our existing GDPR Data Protection Policy (available on our website) and Information Security Policy. For data security Crowcon have a nominated Data Protection Officer who can be contacted via GDPR@crowcon.com

Security Awareness

Q; Please explain how you ensure security awareness among your employees & how you perform screening activities during hiring?

A; Security awareness training is mandatory for all Crowcon employees; this training is provided by Halma with new modules distributed to all employees for completion on a monthly basis. New employees are required to complete core modules when hired as part of the standard induction process.

Hosting

Q; Where is your local IT environment located and who manages the environment? If a third party is used, how do you ensure the environment is properly secured?

A; Crowcon's Local IT Environment is based out of UK Headquarters and is managed internally by Crowcon/Halma employees, working to Halma and Crowcon Security Policies.

Q; Please describe where (geographically) the data will be hosted & how you will ensure that EU Data Protection / GDPR requirements will be met.

The system is hosted and manged on the Microsoft Azure cloud instance hosted in Dublin Ireland. The solution sits on a Halma instance on Azure; this has security that is over and above that of Azure. The Azure ecosystem also uses Microsoft Security Principles, which are applied to all Azure instances and environments. We have a standard setup (firewall, patching and pen testing).

Q; Please also describe how you separate tenant data in a multitenant environment - do you encrypt data of each tenant?

A: The portal database on the live server is encrypted and we use TDE (transparent database encryption).

Protection from Malware

Q; Please describe how your local IT environment is protected from malicious activities? How do you prevent, detect and respond to malicious activities?

A; Malicious activities are prevented from spreading inside our system using the security awareness training provided to all employees. To detect and respond to any Malicious activities that occur, Halma have a team that monitors our environments, this team detects and responds to malicious activities and cascade as appropriate. Halma use at least 3 layers of protection from any malicious code entering the systems.

Q; When interfacing remotely with customers, how you protect malicious code spreading to the customer network?

A; Crowcon’s data solution is standalone and does not interact with any customer systems, the data solution also does not interface with any customer system. The Crowcon Data solution is

accessed independently via a web-based portal. As per other responses our hosted solution is monitored and patched on a monthly basis. Halma use at least 3 layers of protection from any malicious code entering the systems, additionally Microsoft's azure based advanced threat protection systems are in place.

Vulnerability management

Q; Do you conduct network and application penetration tests & vulnerability scans of your IT environment? How often? Will you make the results available to us upon request?

A; Crowcon are a wholly owned Halma company (FTSE100 company). Crowcon's data solution is hosted on the Halma MS Azure instance and thus conform to their IT policies.

As such; annual independent penetration testing is conducted with all critical, high and medium risks remediated.

Monthly vulnerability scans are performed against all systems (& associated with the) solution with all issues resolved. We have a minimum monthly patching process for all elements of the service to ensure security patches are applied to, for example, servers and network infrastructure.

The customer is welcome to perform their own testing and assessment upon request. We require that you inform Crowcon and Halma that you are completing this testing.

Crowcon will share results of any of the above tests upon request.

Q; Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?

A; As per the above information, minimum monthly patching is performed as required by Halma IT team.

Subcontracting

Q; Do you hire subcontractors that would be delivering services to our account?

A; All staff working on the the customer account as well as the data solution will typically be in-house (full-time) employees of Crowcon/Halma companies. Where sub-contractors are employed, this is where skill-sets are required that Crowcon/Halma do not already possess are engaged to develop, troubleshoot, fix, migrate or upgrade systems. Elements of the solution that would require sub contracting, would only be from a perspective of carrying out purposes listed above. All sub contractors are heavily screened and are sourced from an approved list within the Halma group of companies. NDR's are placed between Crowcon/Halma and these contractors, including Data Protection (GDPR) and Confidentiality aspects.

Backup

Q; Please describe the data backup, retention, return and deletion policies. Are these in line with the GDPR requirements?

Describe also the data return/deletion clause (exit clause, escrow).

Data backup

- Daily, Weekly, Monthly and Yearly Backup routine to Azure storage within the same datacentre.
- Retention periods for backups; Daily = 40 days, Weekly = 12 Weeks, Monthly = 12 Monthly, Yearly = 3 Years.

The Crowcon data solution holds email addresses and names of employees - this data is input and managed by the customers' operating business, there are no electronic links to other customer systems.

Crowcon and customer have the ability, to update, delete, update this data.

This data is held securely and details if this are documented below.

The system is hosted and manged on the Microsoft Azure cloud instance hosted in Dublin Ireland

GDPR - (from our policy)

You (the customer) may choose to restrict the collection or use of your personal information in the following ways.

We do not sell, distribute or lease your personal information to third parties unless we have your permission or are required by law to do so.

You may request details of personal information which we hold about you under GDPR, please email gdpr@crowcon.com or write to us using the address listed below.

All screens and terminals are not visible except to authorised employees of Crowcon. All employees are required to enter into an Acceptable Use Agreement (CS 008) before they are given access to organisational information.

Manual records are not be left where they can be accessed by unauthorised personnel. As soon as manual records are no longer required, they will be removed from secure archiving and shredded.

Interfaces

Q; Please describe what interfaces does the solution require with other customer systems (according to current plan) & what data is expected to be transferred?

A; There are no interfaces to customer systems, the Crowcon solution is standalone.

Dependent on the implementation an application may have to be installed on a local PC;

This application downloads data from the portable device (gas detector) and sends this data, securely, to the hosted environment.

Data that is downloaded from the devices are; all timestamped, alarm levels, on/off, time waited alarms & gas detector identifier.

Data is then accessed independently via an online web-portal.

Q; In case the solution is interfacing another customer solution, is an interface design technical document available which defines the interfaces in terms of: communication path (source/destination of the communication), communication direction (push data or pull data), encryption protocol (http, AS2, reverse proxy, secure tunnels (IPsec), etc.?

A; Not applicable; the Crowcon solution does not interface to another customer system. The Gas Detector Data is only communicating with the Crowcon App and via an Internet connection to the hosted environment.

Q; Are the interfaces encrypted? If yes, please provide the encryption protocol/mechanism.

A; As above this is not applicable however the solution can be looked at in two elements; data transmission and storage

- Transmission; device data is encrypted before & during transmission from Local Crowcon App to Hosted Environment

- Storage; the database is encrypted and held on MS Azure, i.e. the hosted environment

Change management

Q; Is there separation of environments for developing, testing and production? Does the customer have access to the testing environment to be able to test relevant changes with can impact data before moving to production?

A; There are three environments;

- Development - independent of test and live

- Test environment; hosted on MS Azure

- Live environment; as above hosted on MS Azure

As written, no customer has access to the test environment, software is tested by multiple teams in Crowcon; developer testing, and our test and verification department. We follow a new product development process (for new features) and a deployment of code to live process.

Q; Does the solution track changes done and provide report of changes, like who did the change, who moved the change to production, what date/time?

A; Audit trails and logging will be used to track access and changes. Every user that logs onto our systems has a unique login and thus traceable. For clarity (with timestamp)

- Application logging is in place

- Access (& security logs) logging available from our MS Azure hosting environment

Q; Please describe your internal change management procedures. Is there a link between this process & clients - if yes, describe it?

A; Change management is via a bug tracking system. We document new feature requests or issues reported in field and have traceability to code changes done. (Client can get a report of changes introduced in each version of the software that we release). This process is documented with an internal Change Management Process document.

IT Continuity

Q; Please describe your IT service Continuity and business continuity approach, including redundancy factors. In this description please include your approach to capacity management.

A; Capacity management; the solution is Cloud based and is set up to scale to meet demand - i.e. the Microsoft Azure hosted solution manages this for Crowcon. Crowcon have also built scale into the solution; we use less than 5% of available resource.

Geo-redundancy and geo-replication is considered for future developments based upon the clients requirements for physical location of data. The data we collect is not for real time alarmin or alerting.

Please also see back up of data.

Q; Do you perform Disaster recovery tests? How often?

A; Crowcon have a disaster recovery procedure; this is specific to internal servers and business continuity. This recovery would apply to our development environment.

The data solution is held on the MS Azure hosted instance, this enables the ability to perform Disaster Recovery tests, based upon the clients requirements.

Access Rights Management

Q; Describe your approach to access rights management including both internal & client users.

A; The solution has a roles-based access system, each of these roles has access to specific functions, e.g. read/access-only to the ability to perform moves, adds and changes).

Access levels at Crowcon exist on this basis, with Developers and Admin users having different access rights. Data availability is based upon access rights and the users requirements to view the data.

User identity Management

Q; Is user identity stored in Active Directory, including both internal and external employees?

A; There is no link between the Crowcon data solution and the customer Active Directory. All user ID requirements to be set by customer.

Authentication

Q; Is authentication based on manual username/password?

A; Yes

Q; Is there Single Sign On implemented (SAML) or role-based authentication implemented (SAML2.0)?

A; SAML2.0 Role based authentication is implemented.

Role based access controls

Q; Does the application provides separable roles for end users to restrict their access to the information needed to perform their duties?

A; Crowcon are compliant to the following;

The application provides separable roles for general users, administrators, developers and line-of-business roles. Access control rules are expressed as enterprise for roles rather than for named users.

Q; Similarly, to above, does the application provide separable roles for IT users?

A; Yes

Segregation of Duties (SoD)

Q; Does the application contain Business functions or roles which must not be combined or assigned to the same person, and if so, creates a relevant risk for the organization (e.g. Workflows with approval steps, risk of fraud, operational risk, etc.).

A; SoD regulations do not currently apply to our solution.

Segregation of roles is achieved using access rights management and role based access controls (see above).

Emergency access

Q; Are there critical actions out of normal business operation which require temporal emergency access and monitoring?

A; This is not a critical system. The system downloads data from a detector - this is used for reporting purposes only and not alarming.

The support model is available.

User access reporting

Q; Does the solution have the option to create a user report?

Does this report include roles assignments including history of the assignment?

The solution does not have the ability for clients to create user reports at this time.

These reports are therefore not currently available but can be implemented based on the clients requirements.

Vulnerability management

Q; Do you conduct network and application penetration tests & vulnerability scans of your cloud service? How often? Will you make the results available to the customer upon request? Will you allow the customer to perform independent vulnerability assessment?

A; Crowcon are a wholly owned Halma company (FTSE100 company). Crowcon's data solution is hosted on the Halma MS Azure instance and thus conform to their IT policies.

As such; annual independent penetration testing is conducted with all critical, high and medium risks remediated.

Monthly vulnerability scans are performed against all systems (& associated with the) solution with all issues resolved. We have a minimum monthly patching process for all elements of the service to ensure security patches are applied to, for example, servers and network infrastructure.

The customer is welcome to perform their own testing and assessment upon request. We require that you inform Crowcon and Halma that you are completing this testing.

Crowcon will share results of any of the above tests upon request.

Q; Do you have a capability to rapidly patch vulnerabilities across all of your computing devices, applications, and systems?

A; Yes, As per the above information, minimum monthly patching is performed as required by Halma IT team.