WEM

WEM FAQ on Safety & Security

WEM | WEM.IO

Question 1 – Information Security Policy

What are the information security policy and (ISO) best practices that apply to the services offered to Customers? Which controls are in place to safeguard the information security policy with regard to:

a. Confidentiality – to prevent unprotected data & services (data leaks)

Answer: Hosted in secure environment. No direct access to application or data services. Active protection against most common security risks (such as OWASP top 10).

b. Integrity – to prevent unreliable data & services (damaged or lost data)

c. Availability – to prevent unavailable data & services (system outage, lack of/leaving support personnel)

Answer: Integrity and availability: both the web frontend as the application services run in a high-availability cluster. All mutations in the database are transactional. Referential integrity is enforced in the database. Full transaction logging and centralized backups to a separate location.

d. Accountability – to log access to data & services

Answer: We log the performance and activity of all the components in our platform. Detailed user & access logging can be modeled for specific applications.

e. Change management

Answer: We maintain a CI/CD setup. All updates to our platform go through QA. We run automated regression tests before each release. We maintain a DTAP environment.

f. Incident management

Answer: All customers can create incidents that are logged in our systems. These incidents are monitored and will be resolved in a timely manner. All customers have 24x7 access to the incident information, through the self-dervice portal (my.wem.io).

g. Service level management

Answer: The default service levels re actively monitored by ZoomBIM. Customers can use the self-service portal to monitor their applications as well to see whether they work within the service level agreement specifications.

Question 2 - ISO27001

Is the service provider ISO 27001 certified?

Answer: ZoomBIM is ISO27001 certified through its cloud hosting provider in the Netherlands (CloudVPS). Certificates are provided on receipt.

Question 3 – Access control & Authorization management

How are access control & authorization management conducted and actively monitored for hosted services?

Answer: The hosted services can only be accessed by ZoomBIM personnel. No customers have access to the hosted environment. The actual services that run on the hosted environment, are of course accessible to customers. There are a number of ways this is controlled:

- First of all a WEM account is needed to access the services, in order to build applications, publish applications, etc. All access is logged in our systems.
- For the applications that are built with WEM, the applications themselves need to manage access and authorization. There are several options:
  I. No access control at all. This would mean that an application is accessible to everybody that knows the URL to access the application.
  II. User management. Every application can use the user management software module that WEM provides. This gives basic access control and authorization control. There is basic logging, that can be extended if needed.
  III. Single sign-on. Applications that are built with WEM can use several protocols to implement single sign-on: SAML can be used to integrate with e.g. Microsoft Active Directory or Google G Suite to implement full authorization & authentication control. OAuth can be used to use social networks like LinkedIn, Facebook, Twitter, etc. for authorization control. Logging will be done using any of these authentication providers.

Question 4 – Access to customer data

Which employees have access to Customer data, and what is the purpose of having access?

a. Which access rights and to which data elements?

Answer: Only our DevOps employees have access to the production environment (this is restricted to a max of three employees). They can access all the key components of our platform that deal with providing out services. If needed, these employees can access Customers applications in the development environment, but they cannot access the applications in the production environment.

b. How is Customer data separated from other customers?

Answer: All Customer data will be stored in separate databases, and only the Customer's applications can access its database.

c. Which reporting is available & monitored on access rights, incl. mutations, administrator rights & special accounts?

Answer: If applications need specific reporting, this is easy to implement in the applications themselves, so all required logging can be available.

Question 5 – IP (Intellectual Property)

What has been agreed upon ownership of Customer's content (intellectual property)?

Answer: By default all content is owned by the Customer. This includes the applications as well as the actual data.

Question 6 – Retention Periods
What are retention periods for Customer data? How will Customer data be deleted?
Answer: We store full backups of all databases up to 28 days. Backups older than 28 days are automatically deleted.

Question 7 – Physical protection
Which physical protection is in place for infrastructure that support hosted services to Customers? How is authorized physical access to hardware monitored?
Answer: We only host our platform at providers that don't allow third-party access to their datacenters.
In the Netherlands that is CloudVPS, other providers are Microsoft and Amazon.

Question 8 – Restrictive filtering
Which measures are in place for
trictive filtering (firewall) and dynamic filtering (intrusion detection & prevention systems) against e.g. hacker attacks like viruses, DDOS)?
Answer: We use a firewall and a reverse proxy that handles the web requests before they are sent to the application servers. We have rules and restrictions that every web request must meet before they are forwarded to the application servers.
Using this 'gatekeeper' functionality we can detect and prevent attacks to our services.
For individual applications it is also possible to set of extensive access control, bases on IP addresses or ranges of IP addresses. This can be used to implement whitelist or blacklist approach to restrict/allow access to individual applications/portals.

Question 9 – Vulnerability scanning
How are vulnerability scanning and penetration testing conducted, incl. frequency?
Answer: We periodically run automated pentests on a monthly basis for the WEM platform. It is also possible to run pentests for applications that are built with WEM. These pentests are not being run automatically: they are run based on customer request and at customer expense.

Question 10 – DR (Disaster Recovery)
Is a disaster recovery/contingency plan in place? Are disaster recovery tests executed on a periodic basis?
Answer: Yes, there is a disaster recovery plan in place. Our backups are tested at least twice a month. We also have a separate disaster recovery environment that is part of our ESCROW arrangement (stichting WEM waarborg).

Question 11 - GDPR

What is the procedure to comply with the European General Data Protection Regulation (GDPR), and especially with the notification of data leaks?

- Which data protection/privacy legislation & ISO norms applies to the services offered to Customers?
- What is the information security incident procedure?
- What is the notification procedure for data leaks?
- Are external suppliers subcontracted to provide the services offered to Customers?

Answer: ZoomBIM has performed extensive GAP analyses which resolved in several technical and organizational measures in order to fully comply to GDPR regulations.

Data protection / privacy legislation & ISO:

- ZoomBIM uses CloudVPS ISO for data protection;
- Besides that employees are informed of privacy procedures as part of the 'Handbook of employee Rules';
- Employees have a standard NDA within their employee contract;
- WEM offers the possibility to sign a 'Processor Agreement'

Incident procedure: all personnel are informed on the incident procedure which funnels the incidents to our support department. Each incident will be treated individually according to set priority

Data Leak: All data leaks are reported and stored for report purposes. By law, data leaks will be reported to the proper authority (Autoriteit Persoonsgegevens). All other concerned parties will be notified according to our standard procedure. all deviations can be included in the processors agreement.

External suppliers: ZoomBIM uses external suppliers to model its projects, by default. External parties are used only in agreement with ordering party.

Question 12 – Certificate protection

Which measures are in place to protect certificates for hosted services to Customers?

Answer: The X509 server certificates are generated and stored on the NGINX webservers that serve as both a reverse proxy and a TLS termination proxy. A CSR is sent to a CA, the private keys do not leave the NGINX servers (we run multiple NGINX servers in a HA cluster). The certificates are renewed every three months.

Question 13 – Security Responsibilities

Which contract clauses are in place to define security responsibilities between service provider and Customers?

a. The right for Customers to receive a proof of a regular audit of the security level of the service provider's solution (at least one security audit per year). The service provider should provide the proof about the audit by independent authority.

Answer: There is at least one annual audit, performed by an external party. Ad hoc audits can be ordered by clients at their own cost.

b. Are Security weaknesses (vulnerabilities) and their mitigation audited and will results be communicated on request of Customers?

Answer: Yes

c. Will Service provider notify Customers in a timely manner of modifications that could impact the provided services?

Answer: Notifications will only be transferred to customers through ZoomBIM, in a timely manner.

d. Is it assured that no other information will be collected by the service provider than those strictly necessary for the service.

Answer: This is assured by contract and legislation.

e. Service provider will provide the location of the servers processing Customer's data and alert Customers in case of change.

Answer: Servers are located, 3 piers in The Netherlands. ZoomBIM will notify Customers on any changes.

f. Non-disclosure agreement.

Answer: we can provide NDA's and actively work with them. We will also, within reason, signed NDA's offered by customers/partners/distributors.

g. Jurisdiction.

Answer: WEM acts under Dutch law.

Question 14 - Auditing

Which audit arrangements are made for the hosted services?

Answer: We internally perform an annual security audit where we review both our processes and the technology stack.

Question 15 – Exit Strategy

What is the agreed exit strategy, incl. secured data return to Customers and deletion of data?

Answer: When Customers want to exit the WEM platform, all data will be made available. The data is owned by the Customer, so we will work with them to export all data and delete all existing data and applications (the content) of the Customer's application(s).