July 2024

Security report

BIMserver.center

BIMserver.center

Table of contents

Introduction

Today, the security and integrity of data on digital platforms is a must for any organisation managing sensitive information. BIMserver.center is a complete platform for data management and collaboration in architecture, engineering, construction and operation projects, designed with a strong focus on information security and protection. Given the increasing threats and challenges in digital environments, advanced measures have been implemented to ensure data security and operational continuity of our services.

This document details BIMserver.center's security approach, describing the organisational and technical measures implemented to protect user information. It addresses key aspects such as data and infrastructure, access control, physical security, incident management, disaster recovery, API security and platform operations. By adopting the industry's best practices and remaining at the forefront of security technology, this ensures that customers can have confidence in the resilience and reliability of services.

Data and infrastructure

At BIMserver.center, proper data protection and management is essential to guarantee the security and confidentiality of information. This section describes the storage architecture and protection measures implemented to safeguard both personal information and project files, ensuring compliance with current codes and the high availability of the service.

Data storage and protection

BIMserver.center ensures data security through a hybrid cloud-based storage architecture with its own servers as well as external servers in cooperation with OVH as a cloud provider. The project data is divided into private and public information:

- **Private information:** Users' personal information, project details, contributions, their relationships with other users and entities, and access restrictions, as well as information concerning Developers, Education, Corporate and Validation account entities, are stored in a PostgreSQL database located in CYPE's data centre servers in Alicante, Spain.

- **Public information:** All information concerning the project files users upload to the platform for personal or shared use is stored on dedicated servers in OVH's data centres in France.
  (https://www.ovhcloud.com/en-gb/personal-data-protection/)

Compliance and confidentiality

Private information, including personal data and building identification, is physically hosted on servers within the EU, ensuring compliance with European legislation and guaranteeing confidentiality in sensitive processes, such as public procurement.

Data access and privacy control

Access control and privacy are fundamental pillars for maintaining the integrity and confidentiality of the information in BIMserver.center. This section explains the authentication, authorisation and privacy control mechanisms that ensure that only authorised users access information, and details the security measures implemented to protect passwords and manage identities.

Identity management and authentication

BIMserver.center implements robust identity management, authentication and authorisation mechanisms to ensure secure access to information for end users. To access the platform, users must be authenticated with their email address and password via the web, mobile app or other apps connected via the public API. User sessions are unique, protected and expire after a period of inactivity. Failed login attempts are logged and trigger temporary blocks to prevent brute-force attacks.

Information access control

BIMserver.center users can specify the level of access and visibility of the different project contributions. The owner and authorised persons can restrict the public viewing of these projects and contributions at any time.

Furthermore, some BIMserver.center employees are authorised to handle, view, modify and delete information stored on the servers of the different platforms. To do so, employees must sign a confidentiality document. The information they have access to will be strictly restricted to the information they need to carry out their work, as well as the maintenance, revision, administration, support, commercial and verification of the information.

Formal processes and responsible persons shall be specified for the deployment of measures in the event of a failure. A responsible person shall be defined to manage and define workers' access to the information.

Password encryption and security

User passwords are encrypted by a secure and non-disclosable method, which is omitted in this document for security reasons. A security mechanism is also defined for the monitoring of user accounts to analyse unusual patterns of behaviour to avoid potential threats to information, such as automatic control of the maximum number of requests in a period from a single session.

Security training

Training is provided to employees as required on information security, business ethics and secure development practices. Including procedures for establishing security roles and responsibilities of staff established by BIMserver.center. Any changes will need to be reflected in the security document.

Physical security of data centres

The physical security of the data centres where the BIMserver.center infrastructure is hosted is crucial to protect against unauthorised access and physical threats. This section addresses the security measures implemented to restrict physical access to servers and ensure the integrity of the infrastructure, including the security procedures adopted at OVH facilities.

Physical access control

Access to the hardware infrastructure of BIMserver.center is under strict control. Only authorised personnel may access it and only for maintenance work. Authorised personnel with access to the hardware will be known and documented. A confidentiality document must also be signed. This access will have sufficient security measures to prevent possible sabotage and to ensure continuous operation.

Security measures include secure locked access for authorised personnel and an alarm connected to a security company, which includes a video surveillance system with image recording for access to servers. There is also a temperature control and monitoring system. Additionally, it includes fire alarm and fire safety measures, such as the appropriate fire extinguishers in the corresponding areas.

Cloud provider infrastructure

Access to the infrastructure of the cloud provider, OVH, follows its own security protocols, guaranteeing the protection of the installations according to its certifications and compliance with European Union standards and codes (more information is available at the following link: OVH Cloud - Security and Compliance).

Incident management and disaster recovery

To ensure operational continuity and minimise the impact of possible incidents, BIMserver.center has implemented robust disaster management and recovery strategies. In this section, we describe the redundant systems, protocols in the event of failures and backup policies that guarantee the rapid recovery of the service in case of any eventuality.

Redundant systems and recovery protocols

To ensure the uninterrupted operation of BIMserver.center, redundant server systems and internet access lines are used. Also, Uninterruptible Power Supply (UPS) systems are used to keep the servers running in case of a power outage.

These measures help to minimise the impact on the service in the event of a hardware component failure. As it is a redundant system with two or more channels, in the event of a specific failure, the operation is ensured with the same security guarantees. In the event of failure, the parts will be replaced by other devices complying with the same security measures as the original ones.

Furthermore, a protocol for action in case of failure is defined, which guarantees a prompt recovery of the system in the event of a failure. The protocol indicates the responsible persons who will be notified if a system failure is detected, in order to repair and recover the system as soon as possible. A risk analysis of the devices has been established and automatic systems for detecting malfunctions and notification via e-mail or SMS to the responsible persons have been set up to ensure continuous and safe operation.

Incident response and management

As a method of incident management and response, rapid response procedures have been implemented for security incidents, including identification, containment, eradication and recovery.

Also, automatic measures have been defined to control failures and notify the responsible persons to guarantee correct operation. External automatic checking systems have also been set up from AWS servers with continuous monitoring of operation and automatic notifications to those responsible via email or SMS in the event of system crashes or failures. Similarly, the systems have been subject to internal audits.

For disaster recovery, several local and remote access mechanisms are established. These mechanisms have been registered in order to identify the measures to be taken in each case. Once the work has been completed, a check is made to ensure that everything is functioning correctly and that all security measures are still active.

In addition, all servers are equipped with strict firewalls that allow only the ports that are essential for their operation to be opened. Antivirus software with automatic updates is also included.

Finally, all incidents are recorded as a follow-up control to avoid future failures, as part of the process of continuous improvement and cumulative knowledge.

Back-up copies

Data backup and storage protocols are defined in locations physically independent of the main data location. Backups will be stored in a secure, protected and isolated way, according to the certifications of the cloud provider (https://www.ovhcloud.com/en-gb/enterprise/certification-conformity). By having redundant systems, copies between them have a one-second replication frequency, in addition to full daily offsite backups.

API security

The BIMserver.center API enables integration with third parties securely and efficiently. This section details the access controls, authorisation mechanisms and security measures implemented to protect communication and data exchange via the API, ensuring that the highest security standards are met.

Access and authorisation controls

The BIMserver.center API ensures that strict access controls and robust authorisation checks are in place to limit potential security breaches. Centralised and secure deferred authentication with Bearer Token-Authentication is used. These controls ensure that the devices validate all object property requests, helping to address any vulnerabilities.

All communication between clients and servers is encrypted via HTTPS connection with an SSL certificate to maintain data confidentiality. Additionally, control mechanisms have been implemented to restrict the use of any application or feature that may override the system's security controls.

The BIMserver.center API implements a structured access control policy, with a clear definition of roles and functions, to ensure correct access to the right users, applying the principle of least privilege. Account management is included, in terms of auditing and deleting inactive accounts, as well as periodic logoff for inactivity. Privileged accounts are strictly monitored.

Resource management and monitoring

To meet and satisfy requests made by users, resource usage limits are implemented and the speed and use of resources are monitored to prevent risks. To this end, the system is continuously monitored by qualified personnel to detect and record attacks, intrusions or unauthorised information disclosures, to prevent resource exhaustion and denial-of-service (DoS) attacks.

Security validation

API security is managed through input validation, the inclusion of URIs in permitted lists and the monitoring of outgoing network traffic to help prevent server-side request forgery.

Network segmentation between web servers and database servers is also established privately to protect the confidentiality and integrity of the requested information.

Regular internal audits and security reviews are conducted to identify and address security misconfiguration issues. There is an automated API inventory via Swagger and continuous monitoring by a manager to maintain endpoint security.

Finally, control measures have been established to detect errors or unauthorised changes in hardware, software and firmware, making the necessary corrections based on official sources.

How the platform works

To ensure that BIMserver.center is operating properly and securely, operational protocols and control measures have been established. This section explains the update policies, performance and load testing, logging and auditing procedures that ensure a stable and secure operation of the system.

Operating protocols

The following measures and protocols are defined to review and ensure the correct operation of the system:

- Those responsible for reviewing and monitoring the correct operation of the platforms are defined.

- The required protocols are established so that, when an error is detected during the operation of the platform, the necessary measures are taken to correct it and transmit the problem to the managers and developers.

- Measures are implemented to review and guarantee the correct operation of the platforms, defining protocols for action, review and periodic testing.

- Vulnerability scans and penetration tests are conducted to prevent theft and ensure data privacy.

- Depending on customers' needs, resource usage and elasticity of the infrastructure are assessed, collecting and storing information for analysis and instance scaling.

- Both performance testing and load testing are carried out, reviewing traffic consumption and CPU usage data and comparing them with the theoretical maximums to assess the system's capacity at times of stress.

Update and patch management

Update, patch and change management policies include procedures for applying security patches and changes to infrastructure and software, maintaining system stability and security. Maintenance windows (at off-peak times) are defined and published in advance. Any changes must be properly logged and published.

Registration and auditing

Mechanisms are enabled to ensure the recording, auditing and traceability of events, operations, actions and activities performed on systems and infrastructures. Records are safeguarded, protected against tampering, modification or unauthorised removal, and are accessible and available to users (if required). Logs are tracked by authorised personnel to ensure that events are properly processed. Finally, an incident log file is established for proper follow-up and identification of improvements.

Privacy and legal issues

Privacy

BIMserver.center is committed to being transparent about how personal customer data is collected and used. For more information, please see BIMserver.center's Privacy Policy.

Terms and conditions

Use of BIMserver.center's services and platforms is subject to the Terms and Conditions of Use, which set out the rules and guidelines for the proper use of our services. These terms ensure that all users understand and accept their responsibilities and rights when using our platforms. For more details, please refer to BIMserver.center's Terms and conditions of use.

Legal notice

BIMserver.center provides information about the legal restrictions and responsibilities related to the use of its services. This notice includes details about intellectual property, disclaimers and other legal issues relevant to users of BIMserver.center. For more information, please review BIMserver.center's Legal notice.

Conclusions

BIMserver.center has a firm commitment to the protection and security of the platform's data. From infrastructure design to operational policies, every aspect is carefully structured to safeguard the integrity and confidentiality of its user information. This is reflected in the implementation of advanced identity management, authentication and access control measures, ensuring that only authorised users can access data.

Furthermore, BIMserver.center is committed to complying with privacy and data protection regulations, especially within the European regulatory framework, ensuring that sensitive information is stored and processed in accordance with applicable laws. This stance not only guarantees data security, but also establishes an environment of trust where users maintain sole control over their information.

In operational terms, the platform implements rigorous incident management and disaster recovery plans to maintain operational continuity and minimise the impact of potential disruptions. This is complemented by clear policies on software updates, performance and load testing, and regular audits to ensure system stability and security at all times.

Through these measures and commitments, BIMserver.center ensures comprehensive data protection with a robust structure and strict policies, prioritising the trust and control of our users.

BIMserver.center© is a service managed by CYPE.
For more information contact info@bimserver.center