Security at Meisterplan

Information Security Statement

We want to earn your trust. That's why we have made IT security, data protection, compliance, and transparency the principles of our work. Learn more about Meisterplan's commitment in our Trust Center.

The security of your data is as important to us as it is to you. Maintaining the confidentiality, availability, and protection of your data assets is our highest priority.

You should be able to trust in a reliable platform and keep control of your data. In order to protect your data, Meisterplan is developed in compliance with high-security standards. Furthermore, Meisterplan (meisterplan.com infrastructures) maintains a robust and comprehensive multi-level security environment. Your data is protected by strict infrastructure and administrative procedures, which are regularly checked by external security experts. For the hosting of your data, we also work with a renowned partner certified according to industry standards.

1. Data Center Security and Redundancy

The Meisterplan application is hosted on AWS EC2 servers in Oregon, USA or Frankfurt, Germany, depending on the data center location selected. The server locations are tested to SOC1 and are ISO27001 certified.

Meisterplan application data is redundantly stored in each region at several isolated server locations to ensure maximum data security and availability. The data centers are continuously monitored.

For compliance details of AWS data centers, please refer to https://aws.amazon.com/compliance/?nc1=h_ls.

Numerous firewall components provide a strong barrier of network security from the internet. Furthermore, we use an AWS service to store and serve backup files.

Meisterplan defends against distributed denial of service attacks (DDos): AWS Shield provides protection against the most common and frequently occurring infrastructure and network attacks that are opposed against web applications.

An intrusion detection software automatically scans for suspicious activities within the hosting center.

2. Data Encryption

In order for you to maintain control of your data, having a strong encryption solution as the strongest component of a multi-level data security strategy is essential.

Meisterplan uses proven TLS technology to encrypt all data transmissions between your device and our servers. Transport Layer Security (TLS) technology is designed to protect your information by establishing trust of our servers through a trusted third party, then by creating a secure channel through which your data can pass to our service, protected from malicious actors. Additionally, the data is AES 256 encrypted via AWS encrypted EBS volumes, commonly referred to as at-rest-encryption.

3. User Authentication

You can control access to your Meisterplan application using advanced authentication solutions. Each user in your Meisterplan environment has a unique user name. We offer forms-based authentication (username and password), Google Sign-In authentication, Microsoft Work Account authentication and Single Sign-On via SAML 2.0. Meisterplan issues a session cookie only to store and transmit encrypted authentication information for the duration of a specific session.

Meisterplan does not use cookies to store other confidential user and session information, but instead implements more advanced security methods based on dynamic data and encoded session IDs. The session cookie does not include the password of the user. All account login attempts are logged, and account lockout policies are automatically applied after a certain number of failed login attempts to prevent brute force attacks.

4. Operational Management

We have implemented policies and procedures designed to ensure that your data assets are secure and backed-up to multiple physical locations. Meisterplan production systems and data can only be accessed by authorized members of the Meisterplan Technical Operations team. We continually evaluate new security threats and implement updated counter-measures designed to prevent unauthorized access or unplanned downtime. Current status and availability of SaaS services can be viewed at any time at https://status.meisterplan.com/.

5. Audit, Penetration Test, Certification According to ISO/IEC 2001:2013 and Assurance

All administrative access to protected data is reviewed on a quarterly basis by internal auditors to confirm that we use it only in the context of responding to customer service matters. Third-party security professionals conduct annual network and application penetration tests to proactively find new attack vectors and security weaknesses, and remedy them immediately.

Here's the latest annual report: Penetration Test (https://meisterplan.com/wp-content/uploads/pdfs/pentest_certificate.pdf)

Meisterplan is also certified according to ISO/IEC 27001:2013, in which compliance with information security standards is controlled and verified by accredited auditors in annual surveillance audits: ISO/IEC 27001:2017 (https://meisterplan.com/wp-content/uploads/meisterplan-iso-27001-certification.pdf)

6. Partners and Suppliers

Meisterplan expects all its partners and suppliers to comply with the highest safety standards. Organizations partnering with Meisterplan are selected via a thorough screening process.

7. Disclosure

In the case of security incidents that affect customer data, Meisterplan maintains a policy of full event disclosure. In the unexpected event of any security incident possibly affecting your data, we will notify your account administrator immediately.

8. Data Security (particularly Art. 32 GDPR)

Meisterplan implements and maintains several technical and organizational measures to protect your data. These measures are in line with and meet the requirements of the German Federal Data Protection Act ("Bundesdatenschutzgesetz") and the General Data Protection Regulation (EU 2016/679). These take into particular account the protection objectives pursuant to Art. 28 Para. 3 Sent. 2 let. c and Art. 32 Para. 1 of the GDPR, such as confidentiality, integrity, and availability of the systems and services, as well as their resilience with regards to the type, scope, circumstances, and purpose of the processing. Details on the implemented technical and organizational measures can be found herehttps://meisterplan.com/terms-of-service/.

9. Engagement

To record any security issue with Meisterplan, to file a security incident report, or if you are concerned or suspect that your Meisterplan identity has been compromised, please contact us without delay at security@meisterplan.com.