Security Policy

Last Updated: March 26th, 2019

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.

All customer data held in Meisterplan is protected by strict infrastructure and administrative procedures. To guarantee the highest levels of physical security and data protection that your organisation requires, Meisterplan (meisterplan.com and meisterplan.net infrastructures) maintains a robust and comprehensive multi-level security environment.

1 Physical Security

The Meisterplan application is hosted on AWS EC2 servers in SOC1-3 tested and ISO27001 certified data centers in Oregon, USA and Frankfurt, Germany. For compliance details of AWS data centers please refer to https://aws.amazon.com/compliance/?nc1=h_ls.

A robust firewall provides a strong barrier of network security from the internet. Furthermore, we use an AWS S3 service to store and serve backup files.

Meisterplan defends against DDoS attacks: AWS Shield provides protection against common and most frequently occurring Infrastructure (layer 3 and 4) attacks like SYN / UDP Floods, Reflection attacks, and others to support high availability of the Meisterplan service.

2 Data Encryption

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

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. Using Google Sign-In or Microsoft Work Account authentication, the username must match the primary email address of the Google or Microsoft Work account. Meisterplan issues a session cookie only to record 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 status.meisterplan.com.

5 Audit 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. Meisterplan contracts with third-party security professionals to conduct network and application penetration testing once per year, to proactively find new attack vectors and security weakness.

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, a notification will be sent to your account administrator.

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 here: https://meisterplan.com/terms-of-service/.

9 Penetration Test and Security Summary Report

Penetration tests against the Meisterplan web application have been and are carried out on a regular basis by third-party security experts. Here's the latest report: https://meisterplan.com/wp-content/uploads/2018/04/Penetration-Test-2018.pdf.

10 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.