MEISTERPLAN

Security Policy

Last Updated: May 15th, 2018

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 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.

5 Data Security Officer

Meisterplan has a permanent and independent internal data security officer as required by paragraph 4 of the German Federal Data Protection Act (»Bundesdatenschutzgesetz«) in the case of data processing of personal data.

6 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.

7 Partners

To the same degree, Meisterplan expects the highest dedication to security standards from all our partners. Organizations partnering with Meisterplan are selected via a thorough screening process.

8 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.

9 German Federal Data Protection Act

Meisterplan implements and maintains several technical and organizational measures to protect your data in accordance with the exacting requirements of the German Federal Data Protection Act (»Bundesdatenschutzgesetz«). These measures are implemented as defined in the annex to section 9 of the »Bundesdatenschutzgesetz« (BDSG).

The following technical and organizational measures required under § 9 BDSG and Annex are taken:

1. Admission access control

In terms of admission access control, the following measures are taken:

☑ *Access control*

☑ *Restricted key distribution*

☑ *Door locking devices*

☑ *Monitoring devices*

2. Machine access control

The following measures related to user authentication are taken:

☑ *Password security (e.g. periodical change of passwords, minimum number of characters, requirements with regard to uppercase letters, lowercase letters, numbers and symbols)*

☑ *Automated pausing after a period of inactivity (e.g. password)*

☑ *Creation of a user master record per user*

3. Data access control

The authorization scheme and access rights are implemented in accordance with their logging requirements:

☑ *Dedicated access levels (profiles, roles, transactions and objects)*

☑ *Evaluation*

☑ *Notice*

4. Transmission control

All measures are taken to ensure that personal data cannot be read, copied, modified or removed without authorization during electronic transmission or transport.

Items to be considered with regard to personal data: measures during transmission, transport and storage of personal data (manually or electronically); verification:

☑ *Encryption / VPN (Virtual Private Network)*

☑ *Logging*

5. Input control

All measures are taken to ensure that it is possible to check and establish whether and by whom personal data have been input into data processing systems, modified or removed.

The verification and documentation of data processing is ensured by:

☑ *Logging and analyses systems*

6. Job control

All measures are taken to ensure that data are processed strictly in accordance with the principal.

☑ *Unambiguous contract design*

☑ *Formalized placing of order to process personal data*

7. Availability control

Personal data are protected from accidental destruction or loss by

☑ *Backup facilities*

☑ *Mirroring disks, e.g. RAID technology*

☑ *Uninterrupted power supply units (USVs)*

☑ *Separate storage of data*

☑ *Anti-virus measures / firewall technology*

8. Separation control

Data collected for different purposes will be processed separately. Measures taken are

☑ Internal multi-tenant capability / appropriation

☑ Function separation / productive environment / test environment

10 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

11 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 support@meisterplan.com.