TAO Security

Please review the TAO security controls. If you have any questions, please contact the TAO Customer Success team or security@taotesting.com.

Organizational Security

- **Information Security Program**
  - We have an Information Security Program in place that is communicated throughout the organization. Our Information Security Program follows the criteria set forth by the SOC 2 Framework. SOC 2 is a widely known information security auditing procedure created by the American Institute of Certified Public Accountants.
- **Third-Party Audits**
  - Our organization undergoes independent third-party assessments to test our security and compliance controls.
- **Third-Party Penetration Testing**
  - We perform an independent third-party penetration at least annually to ensure that the security posture of our services is uncompromised.
- **Roles and Responsibilities**
  - Roles and responsibilities related to our Information Security Program and the protection of our customer's data are well defined and documented. Our team members are required to review and accept all of the security policies.
- **Security Awareness Training**
  - Our team members are required to go through employee security awareness training covering industry standard practices and information security topics such as phishing and password management.
- **Confidentiality**
  - All team members are required to sign and adhere to an industry standard confidentiality agreement prior to their first day of work.
- **Background Checks**
  - We perform background checks on all new team members in accordance with local laws.

Cloud Security

- **Cloud Infrastructure Security**
  - All of our services are hosted with Amazon Web Services (AWS) and Google Cloud Platform (GCP). They employ a robust security program with multiple certifications. For more information on our provider's security processes, please visit [AWS Security | GCP Security].

- **Data Hosting Security**
    - All of our data is hosted on Amazon Web Services (AWS) & Google Cloud Platform (GCP) databases. These databases are all located in the [United States]. Please reference the above vendor specific documentation linked above for more information.
- **Encryption at Rest**
    - All databases are encrypted at rest.
- **Encryption in Transit**
    - Our applications encrypt in transit with TLS/SSL only.
- **Vulnerability Scanning**
    - We perform vulnerability scanning and actively monitor for threats.
- **Logging and Monitoring**
    - We actively monitor and log various cloud services.
- **Business Continuity and Disaster Recovery**
    - We use our data hosting provider's backup services to reduce any risk of data loss in the event of a hardware failure. We utilize monitoring services to alert the team in the event of any failures affecting users.
- **Incident Response**
    - We have a process for handling information security events which includes escalation procedures, rapid mitigation and communication.

Access Security

- **Permissions and Authentication**
    - Access to cloud infrastructure and other sensitive tools are limited to authorized employees who require it for their role.
    - Where available we have Single Sign-on (SSO), 2-factor authentication (2FA) and strong password policies to ensure access to cloud services are protected.
- **Least Privilege Access Control**
    - We follow the principle of least privilege with respect to identity and access management.
- **Quarterly Access Reviews**
    - We perform quarterly access reviews of all team members with access to sensitive systems.
- **Password Requirements**
    - All team members are required to adhere to a minimum set of password requirements and complexity for access.
- **Password Managers**
    - All company issued laptops utilize a password manager for team members to manage passwords and maintain password complexity.

Vendor and Risk Management

- **Annual Risk Assessments**

    - We undergo at least annual risk assessments to identify any potential threats, including considerations for fraud.
- **Vendor Risk Management**
    - Vendor risk is determined and the appropriate vendor reviews are performed prior to authorizing a new vendor.

Contact Us

If you have any questions, comments or concerns or if you wish to report a potential security issue, please contact security@taotesting.com.