Ideate Software Data Security Policies

- **Access and Access Monitoring**

  Access to customer data is limited to Ideate personnel who need access to perform their job duties. Access to customer data is strictly logged. Formal role-based access controls, limiting access to system and system components, are created and these are enforced by the access control system. When formal role-based access controls are not possible, authorized user IDs with two factor authentication are used.

- **Physical Security**

  The servers on which customer data is stored are located at an industry-recognized third-party cloud service provider, with industry standard physical security practices.

- **Password Security**

  Multi-factor authentication is required to access Ideate's production environment. Where multi-factor authentication is not possible, Ideate follows the following password standards:

  - A minimum length of 8 characters
  - At least one lowercase letter
  - At least one number
  - At least one non-alphanumeric character

- **Endpoint Security**

  Antivirus software is required to be installed on all Ideate personnel workstations.

- **Network Security**

  Ideate's data resides on a business level Dropbox and Netsuite access with appropriate security.

- **Security Training**

  All employees are encouraged to participate in helping secure our customer data and company assets.

- **Backups**

  Ideate maintains contemporaneous backup that can be recovered immediately at any point in time unless during a disaster.

Ideate Software Data Security Policies

- **Encryption**

  Data at rest is encrypted with AES 256. All data transmitted between Ideate and users is protected using Transport Layer Security (TLS) and HTTP Strict Transport Security (HSTS). Netsuite SOC1, SOC2 and ISO 27001 auditing compliance.

- **Code Analysis; Vulnerability and Patch Management**

  As part of application security input, there are peer review, and testing prior to validating the code to production. Ideate uses manual source code that is subjected to automated analysis. All identified vulnerabilities are assigned to an owner, tracked, and remediated according to Ideate internal policies.

- **Production Environment**

  Ideate maintains a staging environment for testing, separate from its production environment.

- **Asset Management**

  All company devices and physical assets in the production environment are strictly monitored.

- **Incident Response**

  When an incident is identified, a security incident ticket is created with the details of the event, including date and time the incident occurred, the nature of the incident, and how the incident impacts customers. The creation of that case triggers the notification of appropriate security team members. These team members will immediately initiate an investigation to assess the scope and impact of the situation, and to determine the actions necessary for mitigation.