Pinwheel

Information Security Overview

Introduction

Pinwheel considers protection of Customer Data to be a top priority. As further described in this Pinwheel Information Security Overview, Pinwheel uses commercially reasonable organizational and technical measures designed to prevent unauthorized access, use, alteration or disclosure of Customer Data stored on systems under Pinwheel's control. Pinwheel maintains these security measures in accordance with our SOC 2 Type 2 and ISO 27001 certifications.

1. Customer Data and Management. Pinwheel limits its personnel's access to Customer Data as follows:

1.1. Requires unique user access authorization through secure logins and passwords, including multi-factor authentication for Cloud Hosting administrator access and individually-assigned Secure Socket Shell (SSH) keys for external engineer access;

1.2. Limits the Customer Data available to Pinwheel personnel on a "need to know" basis;

1.3. Restricts access to Pinwheel's production environment by Pinwheel personnel on the basis of business need;

1.4. Encrypts user security credentials for production access; and

1.5. Pinwheel logically separates each of its customers' data and maintains measures designed to prevent Customer Data from being exposed to or accessed by other customers.

2. Data Encryption. Pinwheel utilizes industry-standard encryption for Customer Data as follows:

2.1. Implements encryption in transport and at rest;

2.2. Uses strong encryption methodologies to protect Customer Data, including AES 256-bit encryption for Customer Data stored in Pinwheel's production environment; and

2.3. Encrypts all Customer Data located in cloud storage while at rest.

3. Network Security, Physical Security and Environmental Controls

3.1. Pinwheel uses firewalls, network access controls and other techniques designed to prevent unauthorized access to systems processing Customer Data.

3.2. Pinwheel maintains measures designed to assess, test and apply security patches to all relevant systems and applications used to provide the Services.

3.3. Pinwheel monitors privileged access to applications that process Customer Data, including cloud services.

3.4. The Services operate on Amazon Web Services ("**AWS**") and are protected by the security and environmental controls of Amazon. Detailed information about AWS security is available at https://aws.amazon.com/security/ and http://aws.amazon.com/security/sharing-the-security-responsibility/. For AWS SOC Reports, please see https://aws.amazon.com/compliance/soc-faqs/.

3.5. Customer Data stored within AWS is encrypted at all times. AWS does not have access to unencrypted Customer Data.

4. Independent Security Assessments. Pinwheel periodically assesses the security of its systems and the Services as follows:

4.1. Annual detailed security and vulnerability assessments of the Services conducted by independent third-party security experts that include a code analysis and a comprehensive security review. Pinwheel shall attest to Customer the date of the most recent security and vulnerability assessment at Customer's reasonable request.

4.2. Pinwheel hires accredited third parties to perform audits and to attest to various compliance and certifications annually including SOC 2 Type 2.

4.3. Bi-annual penetration testing of Pinwheel systems and applications to test for exploits including, but not limited to, XSS, SQL injection, access controls, and CSRF.

4.4. Weekly vulnerability scanning.

4.5. Automated analysis of open-source software packages and their dependencies to identify risks in the software supply chain through CI/CD integration.

5. **Incident Response**. If Pinwheel becomes aware of unauthorized access or disclosure of Customer Data under its control (a "**Breach**"), Pinwheel will:

5.1. Take reasonable measures to mitigate the harmful effects of the Breach and prevent further unauthorized access or disclosure.

5.2. Upon confirmation of the Breach, notify Customer in writing of the Breach without undue delay. Notwithstanding the foregoing, Pinwheel is not required to make such notice to the extent prohibited by Laws, and Pinwheel may delay such notice as requested by law enforcement and/or in light of Pinwheel's legitimate needs to investigate or remediate the matter before providing notice.

5.3. Each notice of a Breach will include:

5.3.1. The extent to which Customer Data has been, or is reasonably believed to have been, used, accessed, acquired or disclosed during the Breach;

5.3.2. A description of what happened, including the date of the Breach and the date of discovery of the Breach, if known;

5.3.3. The scope of the Breach, to the extent known; and

5.3.4. A description of Pinwheel's response to the Breach, including steps Pinwheel has taken to mitigate the harm caused by the Breach.

6. Business Continuity Management

6.1. Pinwheel maintains an appropriate business continuity and disaster recovery plan.

6.2. Pinwheel maintains processes to ensure failover redundancy with its systems, networks and data storage.

7. Personnel Management

7.1. Pinwheel performs employment verification, including proof of identity validation and criminal background checks for all new hires, including contract employees, in accordance with applicable law.

7.2. Pinwheel provides training for its personnel who are involved in the processing of the Customer Data to ensure they do not collect, process or use Customer Data without authorization and that they keep Customer Data confidential, including following the termination of any role involving the Customer Data.

7.3. Pinwheel conducts routine and random monitoring of employee systems activity.

7.4. Upon employee termination, whether voluntary or involuntary, Pinwheel immediately disables all access to Pinwheel systems, including Pinwheel's physical facilities.