PRODUCT
LABS

Data Security Measures

This document describes the technical and organizational measures we have adopted and will adopt to ensure that the data we process is safe in our care.

1. Security Measures

PRODUCT LABS has implemented and will maintain appropriate technical and organizational security measures to protect customer personal data from security incidents and to preserve the security and confidentiality of the customer personal data ("**Security Measures**"). The Security Measures applicable to the Services are as follows:

1) Third Party Security Audit: PRODUCT LABS shall continue to be annually audited against the SOC 2 Type II standard. The audit shall be completed by an independent third-party. Within thirty days after any customer's written request, we will provide a copy of the resulting annual audit report.

2) Web Application Penetration Test: PRODUCT LABS shall continue to annually engage an independent, third-party to perform a web application penetration test. Upon any customer's written request, we will provide the executive summary of the report to Customer. We will address all medium, critical and severe vulnerabilities in the findings of the report within a reasonable, risk-based timeframe.

3) Security Awareness Training: PRODUCT LABS will provide annual security training to all personnel. "Security Training" shall address security topics to educate users about the importance of information security and safeguards against data loss, misuse or breach through physical, logical and social engineering mechanisms. Training materials will address industry standard topics which include, but are not limited to:

   • The importance of information security and proper handling of PII

   • Physical controls such as visitor protocols, safeguarding portable devices and proper data destruction.

   • Logical controls related to strong password selection/best practices.

   • How to recognize social engineering attacks such as phishing.

4) Vulnerability Scan: PRODUCT LABS shall ensure that vulnerability scans are performed on servers continuously and network security scans are completed at a minimum biannually, in each case using an industry standard vulnerability scanning tool.

5) Employee-Related Policies:

   a. Unauthorized persons will be prevented from gaining physical access to our premises and the rooms where data processing systems are located.

   b. Employees will only be allowed access to resources for tasks assigned to them.

c. We will ensure that all computers processing personal data (including computers with remote access) are password protected, both after booting up and when left, even for a short period.

d. We will assign individual user accounts for authentication.

e. We will only grant system access to our authorized personnel and strictly limit their access to applications required for those personnel to fulfil their specific responsibilities.

f. We will implement a password policy that prohibits the sharing of passwords, outlines procedures to follow after disclosure of a password, and requires that passwords be changed regularly.

g. We will ensure that passwords are always stored in encrypted form.

h. We will have adopted procedures to deactivate user accounts when an employee, agent, or administrator leaves our employ or moves to another responsibility within the company.

i. We will log administrator and user activities.

j. We will process the customer personal data received from different clients so that in each step of the processing the controller can be identified and so that data is always physically or logically separated.

6) Process-Level Requirements: We will implement the following processes to ensure security and privacy:

a. PRODUCT LABS shall implement user termination controls that include access removal / disablement promptly upon termination of staff.

b. Documented change control process will be used to record and approve all major releases in PRODUCT LABS's environment.

c. PRODUCT LABS shall have and maintain a patch management process to implement patches in a reasonable, risk-based timeframe.

d. PRODUCT LABS shall use firewall(s), Security Groups/VPCs, or similar technology to protect servers storing Customer Personal Data.

e. Where PRODUCT LABS handles customer personal data, servers shall be protected from unauthorized access with appropriate physical security mechanisms including, but not limited to, badge access control, secure perimeter, and enforced user provisioning controls (i.e. appropriate authorization of new accounts, timely account terminations and frequent user account reviews). These physical security mechanisms are provided by data center partners such as, but not limited to, AWS, Azure, and Google. All cloud-hosted systems shall be scanned, where applicable and where approved by the cloud service provider.

f. PRODUCT LABS will virtually segregate all Customer Personal Data in accordance with its established procedures. The Customer instance of Services may be on servers used by other non-Customer instances.

g. Whenever an employee or contractor leaves or is terminated, that individual's access to customer user accounts shall be immediately terminated or disabled.

7) Application-Level Requirements

a. PRODUCT LABS shall maintain documentation on overall application architecture, process flows, and security features for applications handling customer personal data.

b. PRODUCT LABS shall employ secure programming techniques and protocols in the development of applications handling customer personal data.

c. PRODUCT LABS shall employ industry standard scanning tools and/or code review practices, as applicable, to identify application vulnerabilities prior to release.

8) Data-Level Requirements

a. Encryption and hashing protocols used for customer personal data in transit and at rest shall be configured to use current NIST approved encryption standards (e.g. SSH, TLS).

b. PRODUCT LABS shall ensure laptop disk encryption.

c. PRODUCT LABS shall ensure that access to information and application system functions is restricted to authorized personnel only.

d. Customer personal data stored on archive or backup systems shall be stored at the same level of security or better than the data stored on operating systems.

9) End User Computing Level Requirements

a. PRODUCT LABS will prohibit the use of removable media for storing or carrying customer personal data. Removable media include flash drives, CDs, and DVDs.

10) Compliance Requirements

a. PRODUCT LABS will implement building access control to control and track access to its networks and other equipment.

b. PRODUCT LABS will, when and to the extent legally permissible, perform criminal background verification checks on all of its employees that provide services to customers prior to obtaining access to customer personal data. Such background checks shall be carried out in accordance with relevant laws, regulations, and ethics.

c. PRODUCT LABS will determine each year which officers and employees within the company will have access to which categories of data and shall review this list annually at the executive level.

11) Personnel. PRODUCT LABS restricts its personnel from processing Customer Personal Data without authorization by PRODUCT LABS as set forth in the Security Measures and shall ensure that any person who is authorized by PRODUCT LABS to process Customer Personal Data is under an appropriate obligation of confidentiality.

12) Security Incident Response. Upon becoming aware of a Security Incident, PRODUCT LABS will notify Customer without undue delay and, in any case, where feasible, within

seventy-two (72) hours after becoming aware. PRODUCT LABS will provide information relating to the Security Incident as it becomes known or as is reasonably requested by Customer to fulfil its obligations as controller and will also take reasonable steps to contain, investigate, and mitigate any Security Incident.

2. Security Incident Response

Upon becoming aware of any incident in which it suspects that unauthorized access has been gained to Product Labs' systems, the executives of the company at the highest levels will be immediately notified.

1) Executives will immediately confer with each other and with legal counsel regarding any security incident to ensure compliance with legal and contractual obligations.

2) We will notify the impacted customer(s) within twenty-four hours after learning of the incident.

3) We will immediately investigate and mitigate any security incident.

4) Product Labs will obtain and maintain reasonable insurance to cover itself for cyber liability.