TINES
INFORMATION SECURITY ADDENDUM

This Information Security Addendum sets forth the administrative, technical and physical safeguards Tines implements to protect Confidential Information, including Customer Content. Tines may update this Information Security Addendum from time to time to reflect changes in Tines's security protocols, provided such changes do not materially diminish the level of security herein provided. Any capitalized terms used but not defined herein shall have the meanings set forth in the General Terms.

1. **Tines Security Program.** Tines's security program complies with generally accepted industry standards regarding security and compliance, and includes numerous administrative, technical, and physical safeguards designed to protect the confidentiality and security of Confidential Information, including Customer Data. Tines continues to update its security program and strategy to help protect Customer Personal Data (as defined under the Data Processing Agreement) and the Services. As such, Tines reserves the right to update this Addendum from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Addendum. Tines maintains a variety of security policies and procedures designed to safeguard and protect Confidential Information and the integrity of Tines's platforms and systems (collectively, the "**Security Policies**"). An example of such Security Policies include:
    - **a.** Acceptable Use Policy
    - **b.** Access Control Policy
    - **c.** Asset Management Policy
    - **d.** Business Continuity and Disaster Recovery Policy
    - **e.** Change Management and Software Development Life Cycle (SDLC) Policy
    - **f.** Code of Conduct Policy
    - **g.** Data Management Policy
    - **h.** Encryption Policy
    - **i.** Incident Response Policy
    - **j.** Information Security Policy
    - **k.** Open Source Policy
    - **l.** Password Policy
    - **m.** Physical Security Policy
    - **n.** Risk Management Policy
    - **o.** Vendor Management Policy
    - **p.** Vulnerability Management Policy
    - **q.** Whistleblower Policy
2. **Ownership and Updates.** Tines's Head of Information Security leads Tines's Security Program, and works with Tines's executive team, including the Chief Executive Officer, to develop, review, and approve the Security Policies. These Security Policies are reviewed on an ongoing basis, and updated as needed, but no less than annually. Additionally, Tines has established a cross-functional group, led by its Chief Executive Officer, that meets on a regular basis to discuss security and privacy matters. The agenda for security and privacy council meetings typically includes a review of recent incidents, security implications of up-coming features and on-going compliance efforts.
3. **Employee Training.** All new employees are required to complete mandatory security training as part of the new hire process. All Tines employees receive annual training to help ensure awareness and compliance with the Security Policies. All Security Policies are readily available to employees via Tines's internal Google Drive. Additional training is provided to certain employees, based on their respective roles and responsibilities.
4. **Background Checks**. Tines performs background checks on new employees at the time of hire in accordance with applicable local laws.
5. **Confidentiality**. Tines has controls in place to maintain the confidentiality of Customer Data. All Tines employees and independent contractors are bound by Tines's internal policies regarding maintaining the confidentiality of Customer Data and are contractually obligated to comply with these obligations.
6. **Security Protocols**.
    - **a. Least Privilege**. Tine's follows the principle of least privilege for access management. Customer and Authorised Users are given the least amount of privilege necessary to conduct day-to-day operations. Information Owners are responsible for reviewing system privileges on a periodic basis and must promptly request revocation of all privileges no longer required by Customers and Authorised Users. The list of who has access to a system is reviewed quarterly.
    - **b. Encryption**. Customer Personal Data (as defined under the DPA) is encrypted at rest and in transit. All laptop computing devices or storage media owned or maintained by Tines must employ whole disk encryption to protect Customer Personal Data regardless of how sensitive this data is.
        - i. **Data in Transit.** Customer Personal Data is encrypted transit using, at a minimum, TLS v1.2.

ii. **Data At Rest.** All devices owned or maintained by Tines employ whole disk encryption to protect Customer Personal Data regardless of data classification. Customer Personal Data stored at rest is encrypted using AES-256 (Advanced Encryption Standard). Tines does not authorise the storage of Customer Personal Data on mobile or mass storage devices.

c. **Password Management**. All user and administrative passwords must be at least 10 characters in length. Longer passwords and passphrases are strongly encouraged. Where possible, password dictionaries should be utilised to prevent the use of common and easily cracked passwords. Passwords must be completely unique, and not used for any other system, application, or personal account. Default installation passwords must be changed immediately after installation is complete.
d. **Two Factor Authentication**. Accounts must be protected by two factor authentication.
e. **Single Sign On ("SSO")**. SSO is required where possible to avoid using passwords.
f. **Endpoint Monitoring**. All Tines-owned devices are protected with endpoint monitoring software. Systems are monitored 24 hours a day, 7 days a week, 365 days a year.
g. **Data Loss Prevention ("DLP").** Tines Security enforces DLP controls to ensure protection of sensitive data.
h. **Phishing / Email Security.** Security controls are implemented to proactively identify suspicious messages before they reach inboxes. All users receive phishing training as part of security awareness with periodic reminders sent on indicators and reporting mechanisms.
i. **Asset and Mobile Device Management**. Assets and assigned owners (i.e. Tines employees) to those assets are tracked, with real-time checks in place for security control enforcement.
j. **Granular Data Control**. Customers are given granular controls to set retention limits for Customer Personal Data.
k. **Secure Code Development.** Tines uses a combination of training and security tools to ensure its code base is secure and following industry standard practices.
l. **Penetration Testing**. Tines conducts annual penetration testing of the Platform by employing outside consultants to identify any potential security issues. Periodic testing may also be performed by qualified Tines Security personnel. Tines maintains a Bug Bounty Program through Bug Crowd, which allows independent security researchers to report potential security vulnerabilities.
m. **Malware Protection.** All Tines systems are configured to be protected from malware threats. Isolated environments, replicated backups, and secure by design architecture is implemented to limit malware and ransomware events.
n. **Access to Production Systems**. Tines restricts access to production systems to a handful of employees. No contractors or third-parties have access to production. Customer Personal Data is prohibited from leaving the Tines production environment. The list of Tines employees with access to production is regularly reviewed. All remote access is reviewed by security.
o. **Disaster Recovery and Business Continuity**. Tines maintains a Business Continuity and Disaster Recovery Plan approved by leadership. Disaster recovery plans are tested at least annually. These tests ensure the Tines backup procedures and plans are working as expected to recover systems and data.
p. **Logging and Monitoring.** Tines centralizes logs for long term storage, detections, and forensics support. Logs are retained for a minimum of 1 year.
q. **Security and Privacy Council**. Security Automation. Tines uses its product to automate many facets of the Tines security programme for scale and visibility.
r. **SOC 2**. Tines's information security program is aligned to the industry accepted framework, SOC2. Tines maintains SOC Type II compliance and undergoes annual audits related to this certification.
s. **Vulnerability Management.** Tines maintains controls and policies to mitigate the risk of security vulnerabilities in a measurable time frame that balances risk and the business/operational requirements. Tines uses a third-party tool to conduct vulnerability scans regularly to assess vulnerabilities in Tines' cloud infrastructure and corporate systems. Tines employs DAST and SAST software to assess our internal code and dependencies, internal infrastructure, and external attack surface. Scans occur in real time as code changes are committed. External scans are configured on a weekly basis. Should such scans identify a vulnerability Tines will patch the vulnerability as defined in Tines' Vulnerability Management Policy.

7. **Incident Response**. Tines maintains security incident management policies and procedures. Tines' Security Incident Response Team (SIRT), composed of senior members of Tines's product and engineering team, assesses all relevant security threats and vulnerabilities and establishes appropriate remediation and mitigation actions. Security logs are stored for 365 days to ensure forensic and security incident investigation support. Tines uses third party tools and subscribes to various security industry alert services to keep abreast of relevant threats, vulnerabilities or alerts from actual incidents. SIRT is charged with assessing, responding, and remediating all identified security issues. In accordance with Tines's DPA, Tines notifies Customers without undue delay after becoming aware of an actual data breach.
8. **Additional Information**. Customers may review additional information relating to Tines's security protocols, as well as download the Tines Security Pack, which includes (i) Tines's SOC2 Type II Report, (ii) results of Tines's most recent vulnerability scan, (iii) Tines's list of Tines security policies and procedures, and (iv) results of a third-party penetration tests, at the following link: https://www.tines.com/security.