TECHNICAL AND ORGANISATIONAL MEASURES

Vodori shall implement and maintain commercially reasonable administrative, technical, and physical safeguards designed to protect Customer Personal Data. Vodori regularly reviews and modifies its security measures to reflect changing technology, laws and regulations, risk, industry and security practices and other business needs. Vodori may make changes to its security measures, so long as the changes do not result in a lesser standard of security.

Such safeguards shall include:

- **IT Security Policy.** Vodori will maintain a written information security policy applicable to all authorized personnel and systems.
- **Training.** Vodori will provide information security awareness training to all employees at least annually.
- **Access Control.** Vodori will maintain an access control policy, procedures, and controls consistent with industry standard practices. Vodori will limit access to Customer's Personal Data to those employees and contractors with a need-to-know.
- **Password Management.** Vodori will maintain a password management policy designed to ensure strong passwords consistent with industry standard practices.
- **Logical Separation.** Vodori will ensure Customer's Personal Data is logically isolated per customer.
- **Networking.** Vodori will ensure network access control mechanisms are designed to prevent network traffic using unauthorized protocols from reaching the systems and applications infrastructure.
- **Encryption.** Customer's Personal Data will be encrypted in-transit and at rest using industry standard encryption technologies.
- **Logging and Monitoring:** Vodori will maintain logging and monitoring controls designed to detect, investigate, and respond to security events. Logs may include authentication events, system and application activity, administrative actions, security alerts, and incident-response records. Logs are access-restricted, monitored for anomalous or suspicious activity, and retained in accordance with Vodori's retention requirements. Vodori maintains a log of security incidents and uses monitoring/alerting tools to notify appropriate personnel of potential security events.
- **Incident Response Plan.** Vodori will maintain an incident response plan that addresses Security Incident handling. Vodori also maintains an event log of security incidents.
- **Backups of Customer Personal Data.** Vodori will maintain an industry standard backup system and backup of Customer's Personal Data designed to facilitate timely recovery in the event of a service interruption.
- **Disaster Recovery and Business Continuity Plans**. Vodori will maintain disaster recovery and business continuity plans consistent with industry standard practices.
- **Malicious Code Protection.** All Vodori systems will run the current version of industry standard antivirus software with the most recent updates available on each workstation. Virus definitions will be updated within a reasonable period following release by the anti-virus software vendor.
- **Vendor Management.** Vodori will maintain the Third Party/Vendor Management Program and oversee the risk and compliance program for vendors, partners and other third parties by assessing and managing the risks assumed by the nature of relationships with vendors, partners and other third parties.
- **Vulnerability Management Controls.** Vodori will maintain a vulnerability management program to identify and resolve security vulnerabilities in a timely manner.
- **Secure Data Centers:** Vodori processing will take place in ISO 27001 certified data centers.

- **Additional Safeguarding Measures**
    - Vodori conducts periodic reviews of our security policies and practices through independent third-party auditing services. Reporting on Controls at a Service Organisation (SOC 2) Audits, as well as continuous compliance monitoring services and other assessments deemed appropriate.
    - Vodori maintains annual penetration tests to identify and resolve foreseeable attack vectors and potential abuse scenarios.