Vendor Security Measures

This document contains the Security Measures Volpara Health Technologies Ltd. and its affiliates (collectively, “Vendor” or “we”) have in place to safeguard the confidentiality, integrity and availability of data. Unless otherwise defined herein, capitalized terms shall have the meaning given to them in an applicable Data Processing Addendum.

Our security measures are designed to safeguard customer data at every stage of processing, protecting it from unauthorized access, accidental loss, or destruction. As part of our ongoing efforts to maintain a robust security posture, we regularly review and update our security practices to meet industry standards, assuring our customers that their personal data is in safe hands.

1. Data Security Practices

Encryption

We take the security of personal data seriously and implement robust encryption practices to provide protection, aligning with industry standards and best practices. Specifically, we use encryption at rest and encryption in transit as part of our comprehensive data protection strategy.

- Data at rest – All customer personal data is encrypted using Advanced Encryption Standard (AES-256) a strong algorithm that provides data being securely stored and protected against unauthorized access.

Personal Data is statistically de-identified using an expert determination method. De-identified data is encrypted during transmission to Microsoft Azure Cloud.

Data Classification

Vendor has a defined data classification system so that data is categorized and handled according to its sensitivity. This includes sensitive data types, each with specific handling and protection requirements with regard to compliance and security.

---

2. Physical Security

Vendor adopts a cloud-first approach, which reduces the amount of personal data and assets stored within our physical premises. Our offices are secured with robust physical security measures, including electronic access and secured zones.

3. Infrastructure Security

Vendor utilizes Microsoft Azure as its cloud service provider for all production systems and customer data. Microsoft Azure data centres comply with Data Protection Laws and other global standards to provide protection and security of personal data. Azure data centres are equipped with robust security measures, including biometric access, 24/7 monitoring, and backup power systems to safeguard the data. Service providers are reviewed regularly.

Virtual Appliance Hardening

Vendor's virtual appliance is hardened to meet the Center for Internet Security Level 1 Benchmark. The Center for Internet Security (CIS) Level 1 Benchmark is a set of cybersecurity best practices designed to help organizations secure their IT systems and reduce their exposure to cyber threats.

4. Personnel Security

We recognize that personnel are a critical element in maintaining data security. We are committed to hiring the right people with the right skillset and training them on the latest security threats. We have the following processes in place:

- Onboarding/Offboarding Process – We use an HRIS system to automate onboarding and offboarding procedures.
- Interviews – Applicants are interviewed by a panel of specialists to ascertain their qualifications, skills, and suitability for the role.
- Background Checks – All employees undergo a background check at hire conducted by a specialized third-party service.
- Information Security Training – Employees receive information security training and privacy training upon hire and refresher training on an annual basis.
- Security Awareness & Education – Our security team regularly communicates with the company, providing updates on emerging threats and conducting simulated phishing attacks to assess and strengthen our defences.

---

5. Application Security

Access Control

In line with the security principles of 'least privilege' and 'just in time' access, staff are granted the minimum level of access required to perform their duties, ensuring they only have access to the resources necessary for their role. Access is granted only when needed and is removed when no longer required. This reduces the risk of unauthorized access and minimizes the exposure of sensitive data.

Multi-Factor Authentication (MFA) is mandatory for all staff accessing production systems.

Penetration Testing

Penetration testing is performed on at least an annual basis or whenever significant changes are made such as system updates, implementation of new technologies or modification to infrastructure. Penetration testing is completed by independent accredited security firms.

Security Event Logging

We have logging in place to track and record access and activities related to sensitive data, meaning potential security incidents can be promptly identified, investigated, and addressed. We use Microsoft's security suite of tools for protecting data and monitoring for potential threats.

---

6. Compliance Frameworks

Vendor undergoes third-party audits and certifications such as ISO27001 to validate the effectiveness of their security processes. This allows our security controls to align with industry standards and provides independent compliance assurance. In addition to external certifications, Vendor conducts internal audits to maintain compliance with relevant regulations and privacy best practices.

---

7. Security Testing Methodologies

Vulnerability Scanning

Vendor implements a comprehensive vulnerability management program to identify, assess, and remediate security vulnerabilities in our systems, networks, and applications. Our vulnerability management process includes regular vulnerability scans. We maintain a proactive approach by regularly reviewing and updating our vulnerability management procedures to stay ahead of emerging threats.

Secure Development

Vendor uses code scanning tools to review the source code during the development phase. These tools help identify common coding vulnerabilities and other issues that could be exploited by attackers. We scan our software for vulnerabilities during the development process. This proactive approach allows security flaws to be detected early in the development process. Our developers follow secure coding guidelines based on industry standards, including the OWASP Top 10, which provides guidance on mitigating the most common security risks in software development. Security reviews are conducted at various stages of the SDLC to assess the application's architecture, design, and overall security posture.

---

8. Access Controls

Database Isolation

We implement strict access control measures to provide for the segregation and security of personal data. Each customer is provided with a dedicated database, ensuring their data is isolated.

Authentication

Active Directory and SAML integration are available for user authentication. User access is restricted to specific IP subnets.

---

9. Incident Response Procedures

Incident Management

We have a robust incident response program with well-defined roles and responsibilities to allow for swift and effective incident management. The program aligns with leading industry standards and sets forth the protocols for identifying and prioritizing security incidents. Our security team is responsible for evaluating the risks and developing appropriate response strategies.

Evidence Collection
The incident response process incorporates secure methods for collecting evidence while maintaining confidentiality during evidence collection.

---

10. IT Security Governance

Information Security Governance
Comprising key executive members to provide oversight of the information security governance structure.