CHAINYARD

an IT People Company

Security Technical and Organizational Measures (TOMs)

V1.0

CONFIDENTIAL

This document and the information set forth herein are the proprietary property of Chainyard and are to be held in confidence. The information presented in this document is subject to revision at any time.

Table of Contents

VERSION LOG

Date	Document Version	Changes	Author
03/08/21	1.0	First draft	Melissa Bracken

1. Introduction

The security-related technical and organizational measures (TOMs) provided below apply to all standard service offerings provided by Chainyard except where the client is responsible for security and privacy TOMs. Evidence of the security measures implemented and maintained by Chainyard may be presented in the form of up-to-date attestations, reports or extracts from independent bodies upon request from the client.

2. Document Management

Chainyard will validate that necessary documentation is in place between Chainyard and the client where Chainyard processes Personal Data covered by GDPR. In case of a change to the defined scope, any change to the processing of Personal Data will be reviewed to determine any impact on required TOMs and other contract exhibits. Third Parties will be identified for client approval with periodic review to validate ongoing adherence to the agreed upon TOMs.

Chainyard will create and maintain the following security and privacy documentation and store them in a central repository with restricted access control:

a) Chainyard Data Processing Policy
b) Technical and Organizational Measures (TOMs)
c) Non-disclosure Agreement (NDA) or Agreement to Exchange Confidential Information (AECI) or similar (as required)
d) Third Party Agreement (as required)
e) European Commission Model Clause (as required)

3. Security Incidents

Chainyard will maintain an incident response plan and follow documented incident response policies including data breach notifications to the appropriate parties without undue delay where a breach is known or reasonably suspected to affect client personal data.

4. Risk Management

Chainyard will assess risks related to the processing of personal data and create an action plan to mitigate identified risks.

5. Security Policies

Chainyard will maintain and follow IT security policies and practices that are integral to Chainyard's business and mandatory for all Chainyard employees, including supplemental personnel. IT security policies will be reviewed periodically and amended as Chainyard deems reasonable to maintain protection of services and content processed therein.

Chainyard will maintain an inventory of personal data reflecting the instructions set out in the Chainyard Data Processing Policy including disposal instructions upon contract closure. Computing environments with resources containing personal data will be logged and monitored.

Chainyard employees will complete security and privacy training annually and certify each year that they will comply with Chainyard's ethical business conduct, confidentiality, and security policies. Additional policy and process training will be provided to persons granted administrative access to security components that is specific to their role within Chainyard's operation and support of the service, and as required to maintain compliance and certifications.

6. Physical Security

Chainyard will implement the physical security of Chainyard facilities as well as take precautions against environmental threats and power disruptions for employees. Access to the server room and controlled areas will be limited by job role and subject to authorized approval.

7. User Access Management

Chainyard will maintain proper controls for requesting, approving, granting, modifying, revoking, and revalidating user access to systems and applications containing personal data. Only employees with clear business needs are given access to personal data located on servers, within applications, databases and/or the ability to download data within Chainyard's network. All access requests will be approved based on individual role-based access and reviewed on a regular basis for continued business needs. All systems must meet Chainyard IT Security Standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources (OSRs).

For clients using the Trust You Supplier (TYS) product, Chainyard will maintain additional controls for user access to client personal data to prevent unauthorized access to client personal data. Access to client personal data is verified for continued employment and re-validated annually for continued business need. Chainyard will limit privileged access to individuals for a limited period, and usage will be monitored and logged. Any shared access will be for a limited period and usage will be monitored and logged as well as revalidated regularly.

8. System and Network Security

Chainyard will employ encrypted and authenticated remote connectivity to Chainyard computing environments and client system unless otherwise directed by the client.

Chainyard will implement TOMs to support the security of the network as well as confirm the availability of computing environments and access to client personal data. Network security includes measures such as firewalls, remote access control via virtual private networks or remote access solutions, network segmentation, and detection of unauthorized or malicious network activity via security logging and monitoring.

Availability of data through business continuity and disaster recovery planning support our documented risk management guidelines. TYS will have defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Backup data intended for off-site storage will be encrypted prior to transport.

9. Controls and Validation

Chainyard will maintain security policies and procedures designed to manage risks associated with the TYS application.

For the TYS application, changes to systems, networks, and underlying components will be documented in the TYS Jira system. This includes a description and reason for the change, implementation details and schedule, expected outcome, and approval by authorized personnel.

10. Media Handling

Chainyard will implement protections to secure portable storage media from damage, destruction, theft or unauthorized copying and the personal data stored on portable media through encryption and secure removal of data when it is no longer needed. Additional similar measures will be implemented for mobile computing devices to protect personal data.

11. Workstation Protection

Chainyard will implement protections on end-user devices and monitor those devices to ensure they are in compliance with the security standard requiring hard drive passwords, screen saver, antivirus software, firewall software, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations.

Chainyard will securely sanitize physical media intended for reuse prior to such reuse and will destroy physical media not intended for reuse.

12. Privacy by Design

Chainyard will incorporate Privacy by Design principles for systems and enhancements at the earliest stage of development as well as educate all employees on security and privacy annually.

13. Threat and Vulnerability Management

*Threat and Vulnerability Management TOMs apply only to clients with Managed Services.

Chainyard will maintain measures meant to identify, manage, mitigate and/or remediate vulnerabilities within the Chainyard computing environments. Security measures include:

- Patch management
- Anti-virus / anti-malware
- Threat notification advisories
- Vulnerability scanning (all internal systems) and periodic penetration testing (Internet facing systems) within remediation of identified vulnerabilities