PURESPECTRUM

Technical and Organizational Measures (TOMs) – Services

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

Document Management

PURESPECTRUM INC. will validate that necessary documentation is in place between PURESPECTRUM INC. and the Client where PURESPECTRUM INC. 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. Sub-processors will be identified for Client approval with periodic review to validate ongoing adherence to the agreed upon TOMs.

PURESPECTRUM INC. will create and maintain the following security and privacy documentation as well as store them in a central repository with restricted access control:

a. DPA and DPA Exhibit

b. Technical and Organizational Measures (TOMs)

c. Non-disclosure Agreement (NDA) or Agreement to Exchange Confidential Information (AECI) or similar (as required)

d. Sub-processor Agreement (as required) e. European Commission Model Clause (as required).

Security Incidents

PURESPECTRUM INC. will maintain an incident response plan and follow documented incident response policies including data breach notification to Data Controller without undue delay where a breach is known or reasonably suspected to affect Client Personal Data.

Risk Management

PURESPECTRUM INC. will assess risks related to processing of Personal Data and create an action plan to mitigate identified risks.

Security Policies

PURESPECTRUM INC. will maintain and follow IT security policies and practices that are integral to PURESPECTRUM INC. ’s business and mandatory for all PURESPECTRUM INC. employees, including supplemental personnel. IT security policies will be reviewed periodically and amend such policies as PURESPECTRUM INC. deems reasonable to maintain protection of services and Content processed therein.

PURESPECTRUM INC. will maintain an inventory of Personal Data reflecting the instructions set out in the DPA and DPA Exhibit, including disposal instructions upon contract closure. Computing environments with resources containing Personal Data will be logged and monitored.

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

Physical Security

Office access control policies are in place for visitors to local offices. There are no local data centers within PureSpectrum Inc. All data are stored in AWS Cloud based servers.

User Access Management

PURESPECTRUM INC. 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 need access to Personal Data located on servers, within applications, databases and/or ability to download data within PURESPECTRUM INC. ’s network. All access requests will be approved based on individual role-based access and reviewed on a regular basis for continued business need. All systems must meet company IT Security Standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources (OSRs).

PURESPECTRUM INC. will limit privileged access to individuals for a limited period of time and usage will be monitored and logged. Any shared access will be for a limited period of time and usage will be monitored and logged as well as revalidated regularly.

System and Network Security

PURESPECTRUM INC. will employ encrypted and authenticated remote connectivity to PURESPECTRUM INC. computing environments and Client system unless otherwise directed by the Client.

PURESPECTRUM INC. will maintain network security 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. Backup data intended for off-site storage will be encrypted prior to transport.

Controls and Validation

PURESPECTRUM INC. will maintain policies and procedures designed to manage risks associated with the application of changes to the Client facing systems.

Media Handling

PURESPECTRUM INC. 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.

Workstation Protection

PURESPECTRUM INC. will implement protections on end-user devices and monitor those devices to be in compliance with the security standard requiring 2-factor authentication, antivirus software, firewall software, unauthenticated file sharing, hard disk encryption and appropriate patch levels. Controls are implemented to detect and remediate workstation compliance deviations.

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

Privacy by Design

PURESPECTRUM INC. 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.

Threat and Vulnerability Management

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

- Patch management
- Antivirus / antimalware
- Threat notification
- Vulnerability scanning (all internal systems) and annual penetration testing (Internet facing systems) within remediation of identified vulnerabilities.