Technical and Organizational Measures (TOMs) – Security Services

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

Document Management

IBM will validate that necessary documentation is in place between IBM Security and the Client where IBM 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.

IBM 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

IBM 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

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

Security Policies

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

IBM 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.

IBM employees will complete security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM'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 IBM’s operation and support of the service, and as required to maintain compliance and certifications.

Physical Security

*****

**Physical Security applies only to Managed Services*

IBM will implement the physical security of IBM facilities including data centers as well as take precautions against environmental threats and power disruptions for Clients with Managed Services. Access to the data center and controlled areas within the data center will be limited by job role and subject to authorized approval.

User Access Management

IBM 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 IBM'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 corporate IT Security Standards and employ security configurations and security hygiene practices to protect against unauthorized access to operating system resources (OSRs).

For Clients with Managed Services, IBM 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 daily for continued employment and re-validated annually for continued business need. IBM 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

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

For Clients with Managed Services: IBM will implement TOMs to support the security of network as well as confirm the availability of computing environments and access to Client Personal Data. 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. Managed Services 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.

Controls and Validation

IBM Security will maintain policies and procedures designed to manage risks associated with the application of changes to the Client systems.

For Clients with Managed or Strategic Integration Services: Prior to implementation, changes to systems, networks and underlying components, will be documented in a registered change request that includes a description and reason for the change, implementation details and schedule, a risk statement addressing impact to the Client, expected outcome, rollback plan, and documented approval by authorized personnel.

Media Handling

IBM 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

IBM will implement protections on end-user devices and monitor those devices to be 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.

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

Privacy by Design

IBM 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

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

IBM will maintain measures meant to identify, manage, mitigate and/or remediate vulnerabilities within the IBM 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