COMCAST BUSINESS

Description of the Technical and Organizational Security Measures implemented by the Data Importer

The following Technical and Organizational Security Measures apply to the following Comcast Business ("Comcast") Service(s): SD-WAN and Managed Services.

More information about Comcast's security measures is available in the Comcast Cybersecurity Information Security Program Summary set forth on the Comcast Business Privacy Center (available at business.comcast.com/privacy). For more information about how a transfer impact assessment (TIA) can be completed for a Comcast Business Service, please see our *TIA Fact Sheet* available at business.comcast.com/privacy.

Comcast will ensure an appropriate level of security, taking into account the nature, scope, context, and purposes of processing and the risks for the rights and freedoms of natural persons, including maintaining the following safeguards to protect Personal Data:

Organizational Safeguards

+ *Security Program*. Comcast has designated an information security team that identifies reasonably foreseeable internal and external risks, assesses the sufficiency of safeguards, and adjusts the security program based on business changes. Comcast reviews risks and prioritizes security-related projects and initiatives.

+ *Security Policies*. Information security policies are made available to relevant personnel and reviewed periodically.

+ *Hiring*. Comcast requires all new personnel to review and agree to its information security and confidentiality policies during the onboarding process for all employees.

+ *Training*. Comcast trains workforce members that have access to Customer Personal Data concerning appropriate privacy and security practices and compliance with Comcast's data protection obligations. Comcast also provides mandatory information security training on an annual basis to designated personnel.

+ *Subprocessors*. Comcast maintains policies to ensure appropriate access to Customer Personal Data in production environments. Comcast requires all Subprocessors that provide technology infrastructure components for Customer Personal Data, to maintain appropriate cybersecurity measures. Comcast policy requires agreements between Comcast and the Subprocessors include appropriate cybersecurity requirements associated with Customer Personal Data.
    - Comcast manages all changes to the provision of services by Subprocessors, including maintaining and improving existing cybersecurity policies, procedures, and controls. Any change to services provided by a Subprocessor are required to go through Comcast's third-party security assessment process.
    - All Subprocessors are vetted though Comcast's vendor management program.
    - All equipment partners and distributors are vetted through Comcast's procurement process.

Physical Safeguards

+ *Access Control*. Comcast's facilities have physical security systems that are monitored by the Security teams. These measures include: (i) key card access monitoring; (ii) video monitoring of all entrance locations to the facilities; (iii) flood alert systems; (iv) temperature monitoring

solutions in IT rooms and closets; (v) annunciation systems for fire drills; (vi) quarterly user access review led by the Security Team; and (vii) management of user access, which is linked to an active account directory. Unauthorized persons are prevented from gaining access to premises, buildings, or rooms, where data processing systems are located which Process Customer Personal Data. Comcast's facilities that Process Customer Personal Data are monitored via video surveillance. Networking and other required equipment are secured in areas restricted only to personnel that require access to provide the Service(s) to Customer. Reception staff are present during business hours at Comcast's facilities. Comcast policy requires visitors to be escorted by Comcast' personnel while visiting the Comcast facilities with access to Customer Personal Data.

+ *Termination of Access Controls*. Comcast terminates access to its facilities when a workforce member is terminated or otherwise is no longer employed by Comcast. Documented processes are in place for the offboarding of such users.

+ *Data Destruction*. Comcast complies with its written policies and procedures with respect to its retention of Customer Personal Data. Based on the data type, Comcast has a process in place to delete data after a predetermined time for each data type in each application. Data retention is based on the content and usage of data as directed by Customer and not determined by the presence of Customer Personal Data. Comcast securely destroys or returns Customer Personal Data in accordance with its Data Processing Agreements and does not maintain data longer than is reasonably necessary for a legitimate business purpose (including providing Services for Customer). Equipment that contains Customer Personal Data shall be erased prior to recycling so that the Customer Personal Data cannot be read or reconstructed.

Technical Safeguards

+ *Data Access Controls*. Comcast has policies and procedures in place designed to ensure that access to Customer Personal Data is within a particular workforce member's scope of duty and access to data and applications is appropriately based on job function (such as by assigning unique enterprise identifier to each user by our identity and access management platform, multifactor authentication, periodic review of access rights and remote access, secure distribution of sensitive credentials and revoking/changing access promptly when employment terminates or changes in job functions occur).

+ *Data Minimization*. Comcasts only collects Customer Personal Data where necessary for the operation of the Service(s), in connection with providing the Services.

+ *User IDs and Passwords*. Comcast manages the issuance of passwords and has a policy to expand the adoption of single-sign on. Comcast also monitors and manages the users that have access to a particular application or product. Credentials for privileged accounts shall follow Comcast's' password complexity requirements. Credentials will not be hardcoded in any system, code, or configuration; rather they shall be stored using a secrets manager. Privileged accounts may include, but are not limited to, domain administrators, enterprise administrators, server administrators, and local firewall or network device administrators. In addition, service accounts often have elevated privileges at an application level. Comcast policy provides that multifactor authentication be used for privileged accounts or requires the implementation of other technical safeguards. When a privileged account is no longer needed it will be de-provisioned.

+ *Anti-malware*. Comcast complies with its malicious code and anti-virus/malware detection standard, which sets forth procedures for implementing malicious code protection on specified systems. Controls are developed, implemented, monitored, and maintained to ensure appropriate notification of malware events and review of malware controls, to prevent compromise of confidentiality, availability, and integrity of the Services.

+ *Security Patches*. Comcast implements standards related to system updates and deployment of security patches on a regular basis. Updates rated as critical shall be evaluated for impact and deployed on an accelerated timeline.

+ *System Security*. Comcast's computers and systems are configured to automatically lock after a period of inactivity. Business systems that are deemed critical by Comcast are backed up; those backups are encrypted. Internal corporate wireless networks are encrypted and require two-factor authentication.

+ *Incident Response*. Comcast complies with its incident management process; a written procedure for responding to Personal Data Breach (including notifying impacted customers and business partners). Comcast tracks the process for implementing the incident management process and controls that must be developed, implemented, monitored, and maintained to ensure documentation is in place, records are regularly reviewed, capabilities are updated and reviewed, and contacts are maintained for reporting of any Personal Data Breach. The security and operations teams regularly test and monitor the effectiveness of key controls, systems and procedures designed to prevent and detect Personal Data Breach. In addition, the security and operations teams maintain continuous support of the Comcast's systems and services and may from time to time, in consultation with the business stakeholders, recommend that additional or alternative measures for tracking and processing monitoring of Personal Data Breach should be implemented. Following the occurrence of any Personal Data Breach, the team will perform a root cause analysis and create a remediation plan designed to prevent similar incidents from occurring in the future. The Comcast's security incident management procedure shall be reviewed at least annually.

+ *Vulnerability Management*. Vulnerability scans are conducted on a regular basis against Comcast's computing environment. Vulnerabilities are regularly reviewed and prioritized for remediation based on severity and assigned a remediation timeline.

+ *Testing*. Comcast's security testing includes testing of primary application components -- both unauthenticated and authenticated, manual and automated penetration testing -- to identify vulnerabilities. Additionally, Comcast monitors several vulnerability/threat intelligence feeds for up-to-date information about current general security issues, technology-specific vulnerabilities, and patch release information.

+ *Encryption*. Comcast utilizes commercially available and industry standard encryption technologies for Customer Personal Data that is being transmitted by the business over public networks (*i.e.*, the Internet) or when transmitted wirelessly, using TLS 1.2 (or higher) encryption in the design of all systems that support the Services.

+ *Resilience and Business Continuity*. Comcast supports the alignment of business continuity and disaster recovery program with industry standards including recovery of time objectives and business continuity plans and implements and maintains its disaster recovery process; a written policy that defines procedures for disaster recovery (including procedures for backup and recovery for in scope systems). Comcast supports redundancy of information processing facilities for disaster recovery purposes. All applications must go through a technology resilience analysis, an online survey that collects information to determine the criticality, potential resiliency risk and high-level resiliency strategy for applications. In addition, applications identified as either core infrastructure or mission critical must have a completed technology continuity plan, which provides expanded details about resiliency strategy and data backup, steps for failover or recovery, communications plans and roles and responsibilities for executing plans. Each release of any new software or hardware goes through the security development lifecycle process to ensure all cybersecurity guardrails are implemented. System backups are configured to ensure that recovery point objectives (RPO) and recovery time objectives (RTO) can be met by Comcast. Data recovery backups are tested at least annually to ensure that the RTOs and RPOs can be achieved. Comcast reviews and validates all established and implemented disaster recovery processes at least annually.

Comcast will use commercially reasonable efforts to confirm that all Subprocessors it permits to access Company's Personal Data will comply with security obligations at least as restrictive as those provided for herein. In the event Comcast identifies any deficiencies in any such Subprocessors' security controls, Comcast will analyze and remediate within reasonable timeframes, commensurate with their severity.

* * *