

Last updated on October 16, 2023

- 1 Scope.** The scope of these terms herein apply to Managed Data (as defined below).
- 2 General Degree of Care.** Comcast will employ commercially reasonable physical, administrative, and technical security controls appropriately tailored to the nature and scope of its activities under the Agreement and of the Managed Data which shall in no instance be less protective than the procedures used to protect its own confidential and proprietary information of a like kind. In all instances, such protective measures will conform to Information Security Standards (as defined below) and laws applicable to us in our performance of the Services.
- 3 Your Obligations.** Unless otherwise provided for in the Agreement, it is Your responsibility to implement appropriate reasonable physical, administrative, and technical security controls designed to protect the security, confidentiality and integrity of Your data including by: (i) encrypting and decrypting data before and after transmission across the connections provided as part of the Services and (ii) using a firewall, IDS/IPS or similar device(s) to protect Your Systems when connecting to the public internet. You acknowledge and agree that other than as provided for herein with respect to Managed Data, nothing herein shall be construed to impose any information security or data security obligations on Comcast related to Your network or Your data, including in each Service Location for which Comcast is providing the Services set forth in the Agreement.
- 4 Data Protection**
 - 4.1 Comcast will process any Customer Personal Data on behalf of Customer only for the purposes specified in the Agreement, associated Sales Order(s) and SOWs, or as set forth on <https://business.comcast.com/privacy>, or as otherwise instructed by Customer. Comcast will not retain, use, or disclose Customer Personal Data for any commercial purpose other than (a) for the limited and specific purposes of providing the Services under the Agreement; (b) for the operational purposes permitted by Applicable Privacy Laws; and (c) to comply with Comcast's legal obligations. Except as instructed by Customer or as otherwise permitted under the Agreement, Comcast will not retain, use, or disclose Customer Personal Data outside of its direct business relationship with Customer or "sell" or "share" (as defined by Applicable Privacy Laws) Customer Personal Data.
- 5 Return or Destruction**
 - 5.1 Upon request, upon termination of the Agreement, Comcast will securely destroy Managed Data in our possession and control. The foregoing obligation will not extend to backup or archival copies of Managed Data that Comcast generates in the ordinary course of business or to the extent required by applicable law or legal obligation.
 - 5.2 After termination of the Agreement, Comcast will not Process Your Managed Data for any purpose other than to store it and will continue to apply security controls consistent with this Appendix to such Managed Data for the duration of its storage.
- 6 Security Incidents**
 - 6.1 Comcast will maintain a plan for appropriate security incident management and response that covers, at a minimum, the unauthorized access, acquisition, or use of (a) Managed Data or (b) any material part of Comcast's Systems that interacts with Your Systems as part of the Services (each, a "Security Incident").
 - 6.2 Comcast will provide notification of a Security Incident as soon as practicable but not more than what is required under applicable law after confirmation of the Security Incident.
 - 6.3 For any Security Incident, Comcast will provide regular updates to You, and will use commercially reasonable efforts to cooperate with You or Your regulators in Your efforts to investigate the Security Incident.
- 7 Vendor Relationships**
 - 7.1 Comcast will use commercially reasonable efforts to confirm that all vendors it permits to access Managed Data will comply with security obligations at least as restrictive as those provided for herein.
 - 7.2 In the event Comcast identifies deficiencies in any such vendors' security controls, Comcast will analyze and remediate within reasonable timeframes, commensurate with their severity.
- 8 Assessment Rights.**
 - 8.1 No more than once annually, and upon thirty (30) days written notice to Comcast, You may assess Comcast's compliance with the obligations herein. Such assessments will: (i) be limited to the Services provided by Comcast under the Agreement, (ii) consist only of responses to industry standard vendor questionnaires (such as the Standard Information Gathering (SIG)) and (iii) be conducted remotely. For the avoidance of doubt, this right does not extend to assessing any other party that Comcast

Comcast Business Information Security Standards

engages. Each assessment (i) will last no more than one-half (1/2) day, (ii) will be held during Comcast's normal business hours and (iii) shall not involve: (a) access to Comcast's Systems or applications, (b) installation or use of any audit software, (c) access to any highly sensitive areas, or (d) access to any other party's information. In no event shall Comcast be required to divulge any information or provide access to any sites, applications, or Systems that would result in a breach of any of its legal or contractual obligations (including any agreements with its customers, licensors, or any other parties). Comcast shall not be required to disclose its internal cost information, documentation of proprietary business practices or internal or external memoranda. Any request for additional time or effort by You in excess of the audits described in this section shall be provided at Comcast's sole discretion and at standard security consulting rates. Notwithstanding the foregoing and in lieu thereof and in full or partial satisfaction of the foregoing obligation (as the case may be), Comcast may provide You with an independent security report conducted of the Comcast Systems used to store Managed Data such as a SOC (Service and Organization Controls) 2 Type II or other industry recognized compliance assessment relating to one or more of the Services.

9 Security Governance

- 9.1 Security Program: Comcast will maintain written information security policies, standards, and procedures that, at a minimum, meet the applicable obligations herein.
- 9.2 Training: Comcast employees providing Services under the Agreement will complete appropriate security awareness and acceptable use training at least annually.
- 9.3 Vulnerabilities
 - 9.3.1 Each Party agrees to reasonably cooperate with the other Party to identify and remediate any material security vulnerabilities that may affect the provision of the Services.
 - 9.3.2 With respect to any such vulnerabilities, each Party agrees to provide periodic updates and a summary of the remediation upon request.
 - 9.3.3 Any material identified vulnerabilities must be prioritized and remediated or mitigated as soon as practicable and in accordance with the Party's policies, which shall, at a minimum, meet Information Security Standards.
- 9.4 General Compliance: Each Party agrees to not bypass or attempt to circumvent the other Party's security controls.

10 Access to Systems. To the extent Comcast has access to Your Systems in the course of performing the Services or its obligations under the Agreement, the following requirements will apply to it:

10.1 System Access

- 10.1.1 Comcast will use reasonable identity and access management processes that meet or exceed Information Security Standards.
- 10.1.2 Comcast will terminate the access of any User or, if unable to terminate directly, will notify You promptly, if a User no longer needs access to a System.
- 10.1.3 Comcast will periodically conduct user access reviews commensurate with the risk of access.
- 10.1.4 Comcast will only access Your Systems to the extent necessary to provide the Services.

10.2 Devices

- 10.2.1 Comcast will implement and maintain reasonable security standards for all Comcast Devices that meet or exceed Information Security Standards, including but not limited to timely patch management and threat detection measures.
- 10.2.2 Comcast will maintain secure device management controls for all mobile Comcast Devices with access to Your Systems. Such controls will include the ability to wipe the device remotely.

10.3 Users

- 10.3.1 You and Comcast are each individually responsible for the acts and omissions of their respective Users.
- 10.3.2 Comcast will implement reasonable measures to confirm that when a Comcast User is no longer necessary to providing the Services, the Comcast User does not retain Your Managed Data, or access to Your Systems.

10.4 To the extent You connect to Comcast Systems, You agree to implement and maintain equivalent controls no less protective than those set forth in this Section 10. For the avoidance of doubt, in such circumstances, references to "Comcast" in this Section 10.1 and 10.2 shall be deemed to refer to You and Section 10.2 shall apply to Your Devices that connect to Comcast Systems.

(Definitions follow on next page)

DEFINITIONS

All defined terms not otherwise defined herein shall have the same definition as set forth in the Agreement and its exhibits.

"Applicable Privacy Laws" means those privacy and data protection laws and regulations that are applicable to Comcast in its provision of the Services.

"Customer Personal Data" means data provided by Customer to Comcast, as defined by Applicable Privacy Laws that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an individual or household. For the avoidance of doubt, Customer Personal Data does not and shall not include any data transmitted over or through the Services or Comcast equipment.

"Device(s)" means computing, storage, or networking devices operated by or on behalf of (i) Comcast that Process Your Managed Data or that are used to perform the Services and (ii) You, when accessing or connecting to Comcast's Systems or Process Comcast data provided to You as part of the Services, as the case may be or the context may require.

"Information Security Standard(s)" means standards prescribed for use by the National Institute of Standards and Technology or aligned with the International Organization for Standardization/International Electrotechnical Commission 27000 series.

"Managed Data" means (i) user authentication credentials, if any, provided to Comcast for Services or for purposes of billing, (ii) any configuration information provided to Comcast in connection with the Services, (iii) any other authentication data for access to Your Systems provided to Comcast in connection with the Services or (iv) any Customer Personal Data, in each case, only to the extent such data is within Comcast's possession and control. For the avoidance of doubt, Managed Data does not and shall not include any data transmitted over or through the Services or Comcast equipment.

"Process" and its cognates means any operation or set of operations that is performed on information, including collection, storage, disclosure, erasure, and destruction.

"Party" means either party to the Agreement. When used, the other Party means the other party to the Agreement. Unless otherwise stated, a reference to a "Party" includes Users and third parties acting on its behalf.

"Services" means all products and services provided by Comcast to You under the Agreement.

"System(s)" means any applications, websites, computing assets, systems, databases, devices, products, or services that (i) Comcast uses to Process Managed Data or that are used to perform the Services or (ii) You use to access or connect to Comcast Systems or Process Comcast data as part of the Services, as the case may be or the context may require. A Party's Systems exclude any of the other Party's Systems.

"User(s)" means any individual, including employees, contractors, and contingent workers, working on behalf of a Party with access to Managed Data, with access to Systems, or involved in providing the Services.

"You" means the party or parties to the Agreement other than Comcast. Unless otherwise stated, a reference to "You" includes Your Users and persons or entities acting on your behalf in receiving the Services, including but not limited to Your agents, and contractors.

* * *