

# Microsoft Customer Agreement

## Financial Services Amendment

This Financial Services Amendment (“Amendment”) is entered into between Customer and the Microsoft Affiliate who are parties to the Microsoft Customer Agreement (the “Agreement”), and the parties agree that this Amendment supplements the Agreement.

Customer is subject to oversight by a Regulator (defined below). In the event that Customer has separately entered into an amendment with Microsoft to help Customer meet its privacy, security and regulatory requirements as an entity subject to oversight by a Regulator, the parties agree that the rights and obligations included in such amendment apply when Customer purchases Online Services (defined below) from a reseller through the Cloud Solution Provider Program and supplement the Agreement. For avoidance of doubt, this extension of rights is for the sole benefit of Customer and applies only to Customer’s use of the Online Services.

If Customer does not have a separate amendment with Microsoft that addresses Customer’s requirements as an entity subject to oversight by a Regulator, the parties agree that the Agreement is amended as follows:

### 1. *Enabling Customer Compliance*

- a. **Effective Access to Data and Business Premises.** As set forth in this Amendment and for clarity and to be consistent with applicable regulations, Microsoft will provide Customer, Customer’s internal and external auditors (both of which are defined as “Customer Auditor” herein) and Customer’s Regulator, with effective access to data related to the activities outsourced to Microsoft, as well as reasonable access to Microsoft’s business premises (see Section 2(b)(ii) and Section 2(c)(iii)). Customer will at all times have direct access to Customer Data, including Customer’s virtual machines and applications deployed in the Online Services. This includes the ability for Customer to conduct vulnerability and penetration testing of Customer’s deployments in the Online Services or other similar testing as applicable to a specific Online Service that Customer is using. For avoidance of doubt, Customer must conduct any testing in accordance with Microsoft’s terms and conditions, which may require, among other things, Customer to provide Microsoft with advance notice of any tests and prohibit Customer from targeting any other Microsoft customer.
- b. **Regulator Right to Examine.**
  - (i) In the event that Customer’s Regulator requests information relating to Customer’s use of the Online Services, Customer will, in the first instance, use the standard features of the Online Services and the information provided to Customer to respond to such request.
  - (ii) In the event that the Regulator requests to examine the Online Services operations and controls in order to meet the Regulator’s supervisory obligations of Microsoft as a service provider of Customer, Microsoft will provide the Regulator with a direct right to examine the Online Services, including the ability to conduct an on-premises examination; to meet with Microsoft personnel and Microsoft’s external auditors; and to access any related information, records, reports and documents. Such activities may take place at Microsoft’s offices, at other locations where activities relating to the Online Services provided to Customer and its Affiliates are performed, and as otherwise requested by the Regulator.
  - (iii) Microsoft will not disclose Customer Data to the Regulator except as described in the General Privacy and Security Terms in the OST, and the Regulator will not be allowed access to data belonging to any other Microsoft customer.

- (iv) Customer will at all times have access to Customer Data using the standard features of the Online Services and may delegate its access to Customer Data to representatives of the Regulator.
  - (v) Customer and Microsoft will be responsible for their own costs associated with any of the activities described in this Section 2(b).
  - (vi) For clarity, Microsoft and Customer will work together to resolve each Regulator request through discussion and interaction between Customer, Microsoft and the Regulator. Microsoft and Customer acknowledge that the provisions relating to the Regulator right to examine are not intended to contravene or interfere with any applicable laws or regulations, and nothing in this section should be construed as an impediment to the Regulator's ability to examine the Online Services.
- c. **Customer Examination, Monitoring and Audits Rights.** To enable Customer to meet its examination, oversight and control, and audit requirements, Microsoft has developed specific rights and processes that provide Customer, and other customers that are subject to oversight by a Regulator, with access to information, Microsoft personnel and Microsoft's external auditors. Such rights and processes are designed to provide Customer with effectively the same access to information and personnel that Microsoft would provide to a Regulator, while preserving Microsoft's ability to operate the Online Services and protect the privacy and confidentiality of other customers' data. Specifically, Microsoft will provide Customer, including Customer Auditor, with the rights described below. The activities described in Section 2(c)(iii) below may occur onsite in Microsoft's offices or at other locations where activities relating to the Online Services are performed.
- (i) **Online Services Information Security Policy.** As set forth in the OST, each Online Service follows a written data security policy ("Information Security Policy") that complies with certain control standards and frameworks. Microsoft will make each Information Security Policy available to Customer, along with descriptions of the security controls in place for the applicable Online Service and other information reasonably requested by Customer regarding Microsoft security practices and policies.
  - (ii) **Audits of Online Services.** On behalf of customers including Customer and Customer's Auditor, as well as any Regulator, Microsoft will cause the performance of audits of the security of the computers, computing environment and physical data centers that it uses in processing Customer Data (including personal data) for each Online Service. Each audit will result in the generation of an audit report ("Audit Report"), as set forth in the OST. Pursuant to the terms set forth in the OST, if Customer requests, Microsoft will provide Customer with each Audit Report.
  - (iii) **FSI Customer Compliance Program.** Customer may participate in the optional FSI Customer Compliance Program at any time under this Agreement, which enables Customer to have additional monitoring, supervisory and audit rights and additional controls over the Online Services as described in Sections 2(c)(iii)(1) - (2) below.
- 1. **Supervisory Access to Online Services Information and Microsoft Personnel.**

    - A. **Additional Microsoft Support.** Through Customer's Premier Support Services engagement, Customer will have access to Microsoft personnel for raising questions and escalations relating to the Online Services.
    - B. **Audit Webcasts.** Subsequent to Microsoft receiving an Online Services Audit Report, Microsoft will invite all FSI Customer Compliance Program members ("Members") to participate in a webcast, hosted by Microsoft, for Members to discuss the results of the audit. Each webcast will include an assessment of whether: (1) the control procedures were suitably designed to provide reasonable assurance that the stated internal control objectives would

be achieved if the procedures operated as designed, and (2) the control procedures operated effectively during the reporting period. Upon request from Members that attend the audit webcast, Microsoft will provide detailed information regarding planned remediation of any deficiencies identified by the audit.

- C. **Significant Events.** Microsoft will provide communications to all Members regarding (1) the nature, common causes, and resolutions of security incidents and other circumstances that can reasonably be expected to have a material service impact on Members' use of the Online Services; (2) Microsoft risk-threat evaluations; and (3) significant changes to Microsoft's business resumption and contingency plans, or other circumstances, that might have a serious impact on Members' use of the Online Services.
- D. **Penetration Testing.** At least annually, Microsoft will conduct third party penetration testing against the Online Services, including evidence of data isolation among tenants in the multi-tenant Online Services. Upon request, Microsoft will provide Members with a summary report of the results of such penetration testing.
- E. **Transparency of Online Services Through Program Events.** Microsoft will make subject matter experts for the Online Services available to all Members through group events such as webcasts or in-person meetings, including an annual summit event. Such events will include a roadmap of planned developments, an opportunity for Members to provide structured feedback and/or suggestions regarding the FSI Customer Compliance Program and its desired future evolution, and reports of significant events (as described in this section). These events will also provide an opportunity for Members to discuss common issues with each other and raise them with Microsoft. The format and frequency of community events may vary over time; provided, that the objectives set forth in this paragraph will be accomplished not less than annually.
- F. **Additional Member Requests for Information.** For Online Services that have been audited pursuant to SSAE 16 SOC 1 Type II and SSAE 16 SOC 2 Type II, as reflected in the OST, Members may request additional information from Microsoft subject matter experts not addressed through the standard features of the Online Services, the provisions in Section 2 or other available resources, on a fee-based per diem basis. In order to respond to any such request, Microsoft will prepare a statement of work with estimated fees, based on a per diem rate of US\$4,000 per day for each Microsoft employee, plus reasonable travel expenses. Members will not be charged the full per diem fee for a Microsoft engineering resource who is needed for only a portion of a single day. Microsoft will only charge fees for work performed on a pro rata basis. Further, Microsoft will not charge fees for any Microsoft employee performing administrative tasks, such as meeting coordination, escorting visitors or document copying. The statement of work must be executed by both parties before work can commence. Invoicing, payment and tax terms will be the same as for Professional Services under the Microsoft Premier Support Services Agreement.

If a Member is not reasonably satisfied by the sufficiency of the information provided by Microsoft employees, the Member may submit a written request to meet with one of Microsoft's external auditors. Microsoft will request that the external auditor that has audited the relevant Online Service meet with the Member to discuss any questions. Any such discussion will be subject to the agreement of the external auditor, will be at the Member's expense, and will be subject to the Member signing confidentiality documentation in form and content satisfactory to the external auditor.

## 2. Ability to Influence the Online Services and Programs – Suggestions for Additional Testing.

Microsoft will provide each Member with advanced details on existing and future certifications, audit plans and scope and will solicit feedback on any potential changes to current certifications. For each Microsoft audit, 100% of the existing controls in scope for that audit type will be subject to testing by the auditor, and the expectation is that all controls for each audit scope will be tested within a 3-year audit cycle. As part of the FSI Customer Compliance Program, each Member may suggest additional controls to be included in a future audit scope. Microsoft will consider each such suggestion and, if not accepted, will provide a reasoned basis for refusal. For any given audit cycle, across all suggestions from all Members, Microsoft will include a minimum of five Member-specified controls (from the existing control set) in the audit instructions and will inform the auditor that these controls were selected by the Members. Compliance with these controls will be validated using tests that are consistent with the type of audit (e.g., ISO or SSAE) undertaken.

If the total number of Members in the FSI Customer Compliance Program exceeds 15, Microsoft will establish an executive committee (“Executive Committee”). For a given audit cycle, the Executive Committee will determine the five controls described above on behalf of all Members. Microsoft may, at its discretion, include additional controls requested by Members.

The Executive Committee will be comprised of at least one representative from each key regulated market with a participant in the FSI Customer Compliance Program. If there are multiple Members from a given market, the Executive Committee member for that market will be determined by (1) majority agreement among the Members from that market that have more than 10,000 active seats in the Office 365 Services or more than US\$500,000.00 annual commitment of Microsoft Azure Core Services, or (2) a regulator having authority over all Members from that market. The key regulated markets shall, at a minimum, include Canada, United States, United Kingdom, France, Germany, Japan and Italy. Microsoft may add key regulated markets or increase the number of Members on the Executive Committee only in consultation with all Members.

For clarity, nothing in this section precludes Members from requesting that new controls or additional details for a given product, feature or Online Service be included in the roadmap for future audits. Microsoft will consider each such request and, if not accepted, will provide a reasoned basis for refusal.

## 3. FSI Customer Compliance Program Conditions and Processes.

- A. **Conditions.** Customer’s participation in the FSI Customer Compliance Program is conditioned on Customer (a) being regulated by a Regulator; (b) maintaining an active, paid subscription to one or more Online Services through the Agreement; and (c) maintaining an active, paid Microsoft Premier Support Services agreement. Customer also must pay a US\$50,000 annual fee for each year Customer participates.
- B. **Onboarding.** If Customer decides to join the FSI Customer Compliance Program, an authorized Customer representative shall notify Microsoft by sending Customer contact information and purchase order details for the annual fee to the following Microsoft email address: [fsicomppro@service.microsoft.com](mailto:fsicomppro@service.microsoft.com).
- C. **Termination.** Customer may terminate its membership in the FSI Customer Compliance Program at any time by notifying Microsoft. Microsoft may terminate Customer’s



membership in the FSI Customer Compliance Program if Customer fails to satisfy any of the conditions set forth in Section 2(c)(iii)(3)(A) above.

#### **4. Security Incident: Limited Reimbursement for Certain Costs**

To the extent that a Security Incident (as defined in the OST) results from Microsoft's failure to comply with its obligations under the Agreement, and subject to the limitations of liability applicable to each Online Service, Microsoft will reimburse Customer for reasonable out-of-pocket remediation costs incurred by Customer in connection with that Security Incident. "Reasonable out-of-pocket remediation costs" consist of (a) actual costs of payments, fines, penalties, sanctions, attorneys' fees, court costs or fees, or other remedies or liabilities, and any interest thereon, imposed by a court, tribunal, arbitration panel, government body or regulatory agency for a Microsoft-caused Security Incident; (b) additional commercially-reasonable out-of-pocket expenses incurred by Customer or its Affiliates to manage or remedy the Microsoft-caused Security Incident including, without limitation, costs associated with restoring, correcting, or repairing the affected Online Service; (c) commercially-reasonable out-of-pocket expenses for legally-required notifications of Customer's end users of the Microsoft-caused Security Incident (but not the costs of any professional third-party services, including those relating to crisis management, public relations or media relations services, which are indirect and consequential damages under the Agreement). Customer must document all such expenditures and, upon Microsoft's request, those expenditures must be validated by an independent, internationally-recognized third party financial services industry expert chosen by both parties. For avoidance of doubt, the costs reimbursed by Microsoft under this paragraph will be characterized as direct damages subject to the limitation on liability in the Agreement, and not as indirect, consequential, special or incidental damages excluded in the Agreement.

#### **5. Customer Termination Rights**

- a. **Termination at the Direction of Regulator.** Customer may terminate an Online Service at the express direction of a Regulator with reasonable notice.
- b. **Termination for Regulatory Compliance.** In the event Customer becomes subject to a new government law, regulation, requirement, decision, order or other ruling that Customer determines it cannot comply with because Customer is using the Online Service(s), Microsoft will discuss with Customer how to accommodate Customer's requirements. The parties may contemplate adding additional products or services, procuring those products or services from a third-party provider, or adding other solutions, each at Customer's expense. If the parties are not able to satisfy Customer's new regulatory requirements, Customer may terminate the applicable Online Service without cause by giving 60 days' prior written notice to Microsoft.

#### **6. Business Continuity of Online Services**

Microsoft acknowledges that Customer may be required by its Regulator to ensure that it is able to continue to carry on its business in the event of (1) regulatory or other legal action impacting Customer or one of its Affiliates; or (2) termination of the Agreement. Microsoft and Customer agree as follows:

- a. **Continuity after Customer Transfer of Rights.**
  - 1) In the event of the insolvency, reorganization, liquidation or some other action impacting Customer or one of its Affiliates, as provided by applicable law or regulation for the financial industry (e.g., "too big to fail", "recovery and resolution", "special administration", and similar regulations and actions), and to the extent required to maintain continuity of Microsoft's provision of the Online Services purchased by Customer under the Agreement, Microsoft will consent to Customer assigning, sublicensing or transferring its rights under the Agreement to (A) one or more of its Affiliates, or (B) a third party that purchases or otherwise succeeds to any or all of the business or assets or equity of

Customer. In each case, the entity to which rights are transferred is the “Transferee,” and Transferee will have access to Customer Data through Microsoft’s standard processes and tools.

- 2) Microsoft will neither terminate the Agreement nor suspend or delay the performance of its obligations under the Agreement, subject to the following conditions:
  - A. The Transferee must pay all fees and charges payable by Customer to Microsoft under the terms of the Agreement for services provided before the transfer and through the renewal or replacement of the Agreement.
  - B. The Transferee and Microsoft will work in good faith to renew the Agreement or, as appropriate, to replace the Agreement with appropriate terms for Microsoft to provide the Online Services to the Transferee.
  - C. If Microsoft and the Transferee cannot agree on terms, as described in clause B, within 12 months after the transfer of rights to Transferee, then Microsoft may terminate the Agreement by providing notice to Transferee.
  - D. The aggregate liability of Microsoft and its Affiliates to Customer, Customer’s Affiliates and the Transferee will not exceed the aggregate liability of Microsoft and its Affiliates under the Agreement.
- 3) In the event the Transferee would like to enter into a new Agreement, the parties will work in good faith to put in place terms that are appropriate in light of the transfer under this Section 5(a).

b. **Continuity after Termination of Agreement.** If the Agreement terminates for any reason, then Customer may elect to extend the Online Services on a month-to-month basis for up to twelve months from the date of termination by providing notice of such election to Microsoft. During such period, Microsoft will continue to provide, and Customer will continue to receive and pay for, the Online Services pursuant to the terms and conditions of the Agreement. In addition, during such period Customer will be able to retrieve its Customer Data through Microsoft’s standard processes and tools. Customer may cancel the extended service by providing a notice of cancellation to Microsoft. Cancellation will be effective at the end of the month following thirty days after Microsoft receives the notice of cancellation.

c. **Reversibility.** In the event of a termination of the Agreement as described in Section 4 and this Section 5 and Customer chooses to migrate to a different online service, Customer may request that Microsoft provide assistance in such transition through Microsoft’s Professional Services Organization at the then-current rates for such services.

Customer may request migration or transition assistance and support from Microsoft’s Professional Services Organization at any time during the extended service period described in Sections 5(a) and 5(b).

## 7. *Miscellaneous*

a. **Confidentiality.** This Amendment, the Information Security Policy, the Audit Reports, and all information regarding and provided through the FSI Customer Compliance Program are Microsoft Confidential Information. Customer may disclose these items to a Customer Auditor or consultant or a Regulator, provided that (1) Customer first redacts all terms that are unrelated to regulatory oversight and approval, including pricing information and order quantities; and (2) other than disclosures to a Regulator, Customer must comply with the Confidentiality terms of the Agreement as if the disclosure was a disclosure of Microsoft Confidential Information by Customer to a Customer Representative.

b. **Term and termination.** Subject to Section 4 and Section 5 above, this Amendment will terminate automatically upon any termination of the Agreement.

Except for changes made by this Amendment, the Agreement identified above remains unchanged and in full force and effect. If there is any conflict between any provision in this Amendment and any provision in the Agreement identified above and any provision in the OST, this Amendment shall control.

