Microsoft Volume Licensing

Amendment to Contract Documents

Agreement Number | | CAS-72112-P3V9C8

This amendment ("Amendment") is entered into between the parties identified on the attached program signature form. It amends the Enrollment or Agreement identified above. All terms used but not defined in this Amendment will have the same meanings provided in that Enrollment or Agreement.

Campus and School Agreement
Custom Terms CTM

1. **Order Requirements:** Notwithstanding anything to the contrary in the Enrollment for Education Solutions regarding "**Order requirements**", the initial order must include Subscription Licenses for at least one of the following Education Platform Products or any combination for an **Organization-wide Count of at least 25.**

M365 EDU A3 PerUsr
M365 EDU A3 Per User for CoreCAL
M365 EDU A5 PerUsr

These minimum requirements are waived if Institution has a Qualifying Enrollment. Institution must submit an order within 30 days of the effective date of the Enrollment. Microsoft may refuse to accept this Enrollment if it has a business reason for doing so.

2. **Price Levels**: Notwithstanding anything to the contrary in the Enrollment regarding "**Price Levels**", Microsoft will invoice Institutions' reseller for **Level B** as long as the minimum Order Requirements identified are attained. Price level will also be applied to additional orders ie. Step-up sku.

   There are no price levels for Additional Products. Institution's price level will not change during the term of the Enrollment or at renewal or extension.

3. **Setting Prices**: The price Institution will pay to license the Products will be determined by agreement between Institution and its Reseller. However, Microsoft will provide the Reseller with pricing at the outset of this Enrollment and will not increase the prices that it charges the Reseller for the Products during the term of the Enrollment.

4. **Invoice for Quoted Price**: The price quoted for this order to Institution's Reseller is a fixed price based on an estimated order submission date. Microsoft will invoice Institution's Reseller based on this fixed price quote. If this order is submitted later than the estimated order submission date, Institution's Reseller will be charged for net new Online Services subscriptions for the period during which these services were not provided. Pricing to Institution is agreed between Institution and Institution's Reseller.

5. **Transitioning FTE licensing model to Education Qualified User licensing model**: All new Enrollments under this Agreement listing a previous Enrollment leveraging the FTE licensing model will have the following concession available to them for a 12-month term only.

   FTE was previously calculated in the following manner:

   Faculty and Staff: Institution's Organization-wide Count must include all Faculty and Staff in its Organization. In calculating its Organization-wide Count, Institution must

count a full-time member of its Faculty and Staff as 1, a part-time member of its Faculty as 1/3, and a part-time member of its Staff as 1/2.

Education Qualified User is defined as: an employee or contractor (except Students) who accesses or uses an Education Platform Product for the benefit of the Institution.

Notwithstanding anything to the contrary in the Agreement or Enrollment, if the increase in Institution's Education Qualified User count is greater than 20% of Institution's last paid FTE count, Institution will be eligible to order the following product or its successor in year 1 only, as long as the quantity ordered is not greater than 50% of the increased count.

M365 EDU A3 Unified ShrdSvr PerUsr EDU Transition
M365 EDU A3 Unified ShrdSvr Per User for CCAL EDU Transition
M365 EDU A3 ShrdSvr PerUsr EDU Trnstn (Original)
M365 EDU A3 ShrdSvr Per User for CoreCAL EDU Trnstn (Orgnl)

Example #1: FTE=100 EQU=130 (delta is >20%)

Customer would be eligible to transact 15 of associated transitions skus along with 115 of their product requirement option listed below. (i.e. M365 A3, M365 A3 for CoreCal)

Example #2: FTE=100 EQU=115 (delta is not >20%)

Customer would not be eligible to transact any transition skus and should be ordering the product requirement option listed below for EQU quantity.

6. **Additional Terms**

This Amendment has been reviewed by the New Hampshire CTO Council ("NHCTO") and its counsel. They have determined that this Amendment complies with Federal and New Hampshire privacy law, including FERPA and RSA 189:65 through 189:69.

The parties agree that the Agreement is amended as follows:

A) Use of Customer Data

Customer Data will be used only to provide Customer the Online Services including purposes compatible with providing those services. Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. As between the parties, Customer retains all right, title and interest in and to Customer Data. Microsoft acquires no rights in Customer Data, other than the rights Customer grants to Microsoft to provide the Online Services to Customer.

B) Security

Microsoft is committed to helping protect the security of Customer's information. Microsoft has implemented and will maintain and follow appropriate technical and organizational measures intended to protect Customer Data against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction.

Security Training. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will use only anonymous data in training.

Microsoft has implemented and will maintain for Customer Data in the Core Online Services the following security measures, which, in conjunction with the security commitments in the OST (including the GDPR Terms), are Microsoft's only responsibility with respect to the security of that data.

Domain	Practices
Organization of Information Security	**Security Ownership**. Microsoft has appointed one or more security officers responsible for coordinating and monitoring the security rules and procedures. **Security Roles and Responsibilities**. Microsoft personnel with access to Customer Data are subject to confidentiality obligations. **Risk Management Program**. Microsoft performed a risk assessment before processing the Customer Data or launching the Online Services service. Microsoft retains its security documents pursuant to its retention requirements after they are no longer in effect.
Asset Management	**Asset Inventory**. Microsoft maintains an inventory of all media on which Customer Data is stored. Access to the inventories of such media is restricted to Microsoft personnel authorized in writing to have such access. **Asset Handling** - Microsoft classifies Customer Data to help identify it and to allow for access to it to be appropriately restricted. - Microsoft imposes restrictions on printing Customer Data and has procedures for disposing of printed materials that contain Customer Data. - Microsoft personnel must obtain Microsoft authorization prior to storing Customer Data on portable devices, remotely accessing Customer Data, or processing Customer Data outside Microsoft's facilities.
Human Resources Security	**Security Training**. Microsoft informs its personnel about relevant security procedures and their respective roles. Microsoft also informs its personnel of possible consequences of breaching the security rules and procedures. Microsoft will use only anonymous data in training.
Physical and Environmental Security	**Physical Access to Facilities**. Microsoft limits access to facilities where information systems that process Customer Data are located to identified authorized individuals. **Physical Access to Components**. Microsoft maintains records of the incoming and outgoing media containing Customer Data, including the kind of media, the authorized sender/recipients, date and time, the number of media and the types of Customer Data they contain. **Protection from Disruptions**. Microsoft uses a variety of industry standard systems to protect against loss of data due to power supply failure or line interference. **Component Disposal**. Microsoft uses industry standard processes to delete Customer Data when it is no longer needed.
Communications and Operations Management	**Operational Policy**. Microsoft maintains security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Customer Data. **Data Recovery Procedures** - On an ongoing basis, but in no case less frequently than once a week (unless no Customer Data has been updated during that period), Microsoft maintains multiple copies of Customer Data from which Customer Data can be recovered. - Microsoft stores copies of Customer Data and data recovery procedures in a different place from where the primary computer equipment processing the Customer Data is located. - Microsoft has specific procedures in place governing access to copies of Customer Data. - Microsoft reviews data recovery procedures at least every six months, except for data recovery procedures for Azure Government Services, which are reviewed every twelve months. - Microsoft logs data restoration efforts, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process. **Malicious Software**. Microsoft has anti-malware controls to help avoid malicious software gaining unauthorized access to Customer Data, including malicious software originating from public networks. **Data Beyond Boundaries** - Microsoft encrypts, or enables Customer to encrypt, Customer Data that is transmitted over public networks. - Microsoft restricts access to Customer Data in media leaving its facilities. **Event Logging**. Microsoft logs, or enables Customer to log, access and use of information systems containing Customer Data, registering the access ID, time, authorization granted or denied, and relevant activity.
Access Control	**Access Policy**. Microsoft maintains a record of security privileges of individuals having access to Customer Data. **Access Authorization** - Microsoft maintains and updates a record of personnel authorized to access Microsoft systems that contain Customer Data. - Microsoft deactivates authentication credentials that have not been used for a period of time not to exceed six months. - Microsoft identifies those personnel who may grant, alter or cancel authorized access to data and resources. - Microsoft ensures that where more than one individual has access to systems containing Customer Data, the individuals have separate identifiers/log-ins. **Least Privilege** - Technical support personnel are only permitted to have access to Customer Data when needed.

Domain	Practices
	- Microsoft restricts access to Customer Data to only those individuals who require such access to perform their job function. **Integrity and Confidentiality** - Microsoft instructs Microsoft personnel to disable administrative sessions when leaving premises Microsoft controls or when computers are otherwise left unattended. - Microsoft stores passwords in a way that makes them unintelligible while they are in force. **Authentication** - Microsoft uses industry standard practices to identify and authenticate users who attempt to access information systems. - Where authentication mechanisms are based on passwords, Microsoft requires that the passwords are renewed regularly. - Where authentication mechanisms are based on passwords, Microsoft requires the password to be at least eight characters long. - Microsoft ensures that de-activated or expired identifiers are not granted to other individuals. - Microsoft monitors, or enables Customer to monitor, repeated attempts to gain access to the information system using an invalid password. - Microsoft maintains industry standard procedures to deactivate passwords that have been corrupted or inadvertently disclosed. - Microsoft uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. **Network Design**. Microsoft has controls to avoid individuals assuming access rights they have not been assigned to gain access to Customer Data they are not authorized to access.
Information Security Incident Management	**Incident Response Process** - Microsoft maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. - For each security breach that is a Security Incident, notification by Microsoft (as described in the "Security Incident Notification" section above) will be made without undue delay and, in any event, within 72 hours. - Microsoft tracks, or enables Customer to track, disclosures of Customer Data, including what data has been disclosed, to whom, and at what time. **Service Monitoring**. Microsoft security personnel verify logs at least every six months to propose remediation efforts if necessary.
Business Continuity Management	- Microsoft maintains emergency and contingency plans for the facilities in which Microsoft information systems that process Customer Data are located. - Microsoft's redundant storage and its procedures for recovering data are designed to attempt to reconstruct Customer Data in its original or last-replicated state from before the time it was lost or destroyed.

C) Educational Institutions

If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA) apply, Microsoft acknowledges that for the purposes of the OST, Microsoft is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Microsoft agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials.

Customer understands that Microsoft may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer will be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Microsoft to students (or, with respect to a student under 18 years of age and not in attendance at a postsecondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Microsoft's possession as may be required under applicable law.

D) Data Retention

At all times during the term of Customer's subscription, Customer will have the ability to access and extract Customer Data stored in each Online Service. Except for free trials, which customer or Microsoft will delete per the terms of the trial software, Microsoft will retain Customer Data

stored in the Online Service in a limited function account for 90 days after expiration or termination of Customer's subscription so that Customer may extract the data. During this period, Microsoft provides multiple notices, so you will be amply forewarned of the upcoming deletion of data. After the 90-day retention period ends, Microsoft will disable Customer's account and delete the Customer Data.

E) Third-party Users

Third-party users of Customer's services have no privity of contract with Microsoft, and must exercise their rights to their own data that may be contained in Customer Data by working directly with Customer. Any third-party seeking to enforce their rights to their own data contained in Customer Data may retain possession and control of their own third-party generated content and may review personally identifiable information and correct erroneous information, by requesting Customer staff assist them in obtaining possession and control, and/or in reviewing/correcting content/information.

F) Parent Access and Student Accounts

Customer shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review personally identifiable information in the pupils records, correct erroneous information, and procedures for the transfer of pupil generated content to a personal account, consistent with the functionality of services. Customer shall be responsible for administering this process. During the term of the enrollment, Microsoft shall maintain access to the data the customer wishes to modify or delete. In the event that Microsoft is contacted by an individual seeking access to personally identifiable information, Microsoft shall, where feasible, refer the individual to the Customer, who will follow the necessary and proper procedures regarding the requested information.

G) Security Incident Notification

If Microsoft becomes aware of any unlawful access to any Customer Data or Support Data stored on Microsoft's equipment or in Microsoft's facilities, or unauthorized access to such equipment or facilities resulting in loss, disclosure, or alteration of Customer Data or Support Data (each a "Security Incident"), Microsoft will promptly (1) notify Customer of the Security Incident; (2) investigate the Security Incident and provide Customer with detailed information about the Security Incident, including, if known, the date or estimated date of the unlawful access and the categories of data affected; and (3) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Incident. Given the nature of the Online Services and Microsoft's privacy policies, Microsoft will generally not have knowledge of the data or categories of data stored by Customer. In the event of unlawful access, Microsoft's ability to provide detailed information about the data accessed may be limited. Microsoft will provide such details about the unlawful access as are reasonably available to it.

Notification(s) of Security Incidents will be delivered to one or more of Customer's administrators by any means Microsoft selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on each applicable Online Services portal. Microsoft's obligation to report or respond to a Security Incident under this section is not an acknowledgement by Microsoft of any fault or liability with respect to the Security Incident.

Customer must notify Microsoft promptly about any possible misuse of its accounts or authentication credentials or any security incident related to an Online Service.

Microsoft will comply with the provisions of New Hampshire's data breach statute (RSA 359-C:19 *et. seq.*), as applicable, in the event of a Security Incident.

H) Applicable Law, Venue and Jurisdiction

This agreement, as amended, is governed by the laws of the State of New Hampshire. The parties agree that any lawsuits that include a claim for money damages against Customer relating to this agreement must be brought in the United States District Court, located in New Hampshire. Any other legal actions relating to this agreement must be brought in a court of competent jurisdiction within federal courts located in the jurisdiction of the state where Customer is organized, and the parties agree that jurisdiction and venue in such courts is appropriate, where prerequisites for federal court jurisdiction are present.

I) Subcontractor Transfer

Microsoft may hire subcontractors to provide certain limited or ancillary services on its behalf. Any subcontractors to whom Microsoft transfers Customer Data, even those used for storage purposes, will have entered into written agreements with Microsoft that are no less protective than required by the Online Services Terms ("OST"). Customer has previously consented to Microsoft's transfer of Customer Data to subcontractors as described in the OST. Except as set forth in the OST, or as Customer may otherwise authorize, Microsoft will not transfer to any third party (not even for storage purposes) personal data Customer provides to Microsoft through the use of the Online Services. Microsoft provides a website that lists subcontractors authorized to access Customer Data in the Online Services as well as the limited or ancillary services they provide. At least 6 months before authorizing any new subcontractor to access Customer Data, Microsoft will update the website and provide Customer with a mechanism to obtain notice of that update. If Customer does not approve of a new subcontractor, then Customer may terminate the affected Online Service without penalty by providing, before the end of the notice period, written notice of termination that includes an explanation of the grounds for non-approval. If the affected Online Service is part of a suite (or similar single purchase of services), then any termination will apply to the entire suite. After termination, Microsoft will remove payment obligations for the terminated Online Services from subsequent Customer invoices.

J) Online Services Information Security Policy

Each Online Service follows a written data security policy ("Information Security Policy") that complies with the control standards and frameworks shown in the table below.

Online Service	ISO 27001	ISO 27002 Code of Practice	ISO 27018 Code of Practice	SSAE 16 SOC 1 Type II	SSAE 16 SOC 2 Type II
Office 365 Services	Yes	Yes	Yes	Yes	Yes
Microsoft Dynamics 365 Core Services	Yes	Yes	Yes	Yes*	Yes*
Microsoft Azure Core Services	Yes	Yes	Yes	Varies**	Varies**
Microsoft Cloud App Security	Yes	Yes	Yes	Yes	Yes
Microsoft Graph	Yes	Yes	Yes	No	No
Microsoft Intune Online Services	Yes	Yes	Yes	Yes	Yes
Microsoft Business Application Platform Core Services	Yes	Yes	Yes	Yes	Yes

**Does not include Microsoft Social Engagement.*

***Current scope is detailed in the audit report and summarized in the Microsoft Azure Trust Center.*

Microsoft will provide an updated schedule for products not shown on this graph via the Online Services Terms document.

Microsoft may add industry or government standards at any time. Microsoft will not eliminate a standard or framework in the table above unless it is no longer used in the industry and it is replaced with a successor (if any). In the event Microsoft provides Customer with products not shown on the schedule above, Microsoft, where appropriate, will provide an updated schedule listing the Microsoft product or service and the applicable control standard via the Online Services Terms document.

Subject to non-disclosure obligations, Microsoft will make each Information Security Policy available to Customer, along with other information reasonably requested by Customer regarding Microsoft security practices and policies.

Customer is solely responsible for reviewing each Information Security Policy and making an independent determination as to whether it meets Customer's requirements.

K) Privacy Terms

Microsoft offers the same privacy protections found in this Amendment between it and Customer to any other local education agency ("LEA") in New Hampshire who enters into an Enrollment under this Agreement.

7. This amendment is effective through **September 30, 2023**. Both parties agree to engage in a good faith effort to renegotiate the terms of the renewal at least 60 days prior to the expiration date listed above.

Except for changes made by this Amendment, the Enrollment or 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 Enrollment or Agreement identified above, this Amendment shall control.

This Amendment must be attached to a signature form to be valid.

Microsoft Internal Use Only:

NHCTO Council New Master Terms CASA Amendment (NH Data Privacy) 06182019.docx	CTM	CTM-CTC-AGR-ENR-CPT-CPC	BD