Anlagen zur Dienstvereinbarung zum Dauerbetrieb von Microsoft 365 an der FernUniversität in Hagen

Anlage 1 - Nutzungsbedingungen

Regelungen zum Einsatz von Microsoft 365 für Nutzende an der FernUniversität in Hagen

Geltungszeitraum

Die Regelungen zur Nutzung von Microsoft 365 (M365) im Dauerbetrieb sind Bestandteil der Dienstvereinbarung. Daher gelten für diese die Regelungen zur Gültigkeit der Dienstvereinbarung nach Ziff. 11 (3).

Geltungsbereich

Diese Nutzungsbedingungen gelten für alle Personen, die über die FernUniversität einen Zugang zu den Anwendungen in M365 erhalten.
Sie sind Bestandteil der Dienstvereinbarung zum Dauerbetrieb von Microsoft 365gelten jedoch ebenfalls für nicht-dienstverpflichtete Personen, soweit sie auf MS 365 Anwendungen über einen FernUniversitäts-Zugang zugreifen

Nutzungszeitraum

Die allgemeine Nutzung der Dienste ist gekoppelt an die Vertragslaufzeit des Rahmenvertrages der FernUniversität mit Microsoft. Der Nutzungszeitraum ist beschränkt auf die Dauer dieses Vertragsverhältnisses, die FernUniversität gibt Änderungen in diesem Verhältnis unverzüglich auf geeignetem Wege bekannt. Mit Zugang der Mitteilung darf die Software bzw. der Dienst nicht mehr weiter genutzt werden und die Software muss gelöscht werden.

Das individuelle Nutzungsrecht ist beschränkt auf den Zeitraum, in dem die Person Mitglied oder Angehörige*r der Hochschule ist oder als externe Person ein Nutzungsrecht eingeräumt bekommen hat.

Lizenzzuweisung

Die FernUniversität weist den Nutzenden zu dienstlichen, universitären oder akademischen Zwecken eine personengebundene Lizenz zu. Die Nutzung für private sowie kommerzielle Zwecke ist nicht erlaubt.

Mit der Lizenzzuweisung erhalten alle Nutzenden einen Microsoft-Account (sog. Schul- und Geschäftskonto). Die Zugangsdaten dürfen in keinem Fall an Dritte weitergegeben werden.

Die Nutzung von Microsoft 365 ist auf allen dienstlichen Geräten erlaubt. Sofern es dienstliche Erfordernisse gibt, ist die Nutzung ausnahmsweise auch auf privaten Endgeräten gestattet. Für private Geräte kann allerdings kein vollumfänglicher Support angeboten werden – es kann nur eine eingeschränkte Hilfe (ohne Remoteunterstützung) durch das ZDI erfolgen.

Anmeldung und Aktivierung

Für die Lizenzaktivierung müssen sich Nutzende mit ihrem FernUni Anmeldenamen und Passwort in den Microsoft-Anwendungen anmelden (Anmeldename@buerokommunikation.fernuni-hagen.de + Passwort).

Nutzbare Microsoft Dienste

Die Nutzung der Microsoft Dienste erfolgt nach den Lizenzbedingungen des Herstellers (Externer Link: Microsoft Product Terms).
Die nutzbaren Microsoft-Dienste und Anwendungen regelt verbindlich Anlage 2 – Verzeichnis der Anwendungen.
Die FernUniversität behält sich vor, der Benutzerin oder dem Benutzer lediglich eine Auswahl an Software und Diensten anzubieten oder einzelne Funktionen der Software und Dienste einzuschränken.

Erläuterung zu den Zugriffsrechten

- Bei dem Microsoft-Account handelt es sich um einen persönlichen dienstlichen Account, der zur Verfügung gestellte Speicherplatz (OneDrive) steht exklusiv zur Verfügung.
- Andere Nutzende haben keinen Zugriff auf den persönlichen Arbeitsbereich. Ein Einsehen der Daten durch andere Nutzer*innen ist nicht möglich, das geschieht erst dann, wenn Daten geteilt werden.
- Sofern Daten im Teams-Umfeld gespeichert werden, hat jedes Team-Mitglied Zugriff auf diese Daten bzw. diesen Team-Bereich. Dieser Bereich ist aber wiederum getrennt von den jeweiligen persönlichen Bereichen der Nutzer*innen.
- Vorgesetzte, Teamleitende etc. erhalten keinen Zugriff auf den Account und den persönlichen Bereich der Nutzenden (Ausnahmen regelt Anlage 5 – Rollen- und Berechtigungskonzept).
- Aufzeichnungen aus Besprechungen werden im Besprechungschat angezeigt und im persönlichen OneDrive des Organisators gespeichert. Zugriff auf diese Aufzeichnung haben die jeweiligen Teilnehmenden der Besprechung sowie der Organisator selbst.
- Die gesondert verpflichteten Administrator*innen des ZDI (Zentrum für

Digitalisierung und IT) haben im Rahmen ihrer dienstlichen Aufgaben administrative Zugriffsrechte (Diese Ausnahme regelt Anlage 5).

Datensicherung / Backup

Es erfolgt eine tägliche Sicherung der Microsoft 365 Plattform, sodass Daten in OneDrive, Teams und Sharepoint regelmäßig gesichert werden. Über einen sog. Serviceaccount sind die Microsoft-Dienste mit dem externen Backup-Dienst verbunden (Keepit-Serviceaccount).

Zusammenarbeit mit externen Personen / B2B-Usern in Microsoft 365

- Externe Personen / B2B-User sind Personen, welche keine Mitarbeitenden der FernUniversität sind (z. B. Dienstleistende, Kooperationspartner). Für diesen Nutzerkreis ist die private sowie kommerzielle Nutzung ausgeschlossen.
- Externe Personen verfügen aus lizenzrechtlichen sowie datenschutzrechtlichen Gründen über einen eingeschränkten Nutzungsumfang. So ist es nur möglich, diese Personen in ein Team einzuladen, um kollaborativ zu arbeiten. Zugriffe auf sonstige Bereiche (z. B. OneDrive) sind nicht möglich. Einladungen zu Besprechungen bzw. die Teilnahme an Besprechungen sind dagegen möglich.
- Diese Personen können von einem verantwortlichen Bereich oder Beschäftigten für das kollaborative Arbeiten als Gäste oder externe Teilnehmer zu Microsoft 365 eingeladen werden.
- Wenn entsprechende Einladungen an Externe notwendig sind aufgrund bestimmter Zusammenarbeit, z. B. in der Forschung oder auf Verwaltungsebene mit anderen Hochschulen, muss dieses angemeldet werden. Hier stellt das ZDI einen entsprechenden Prozess bereit. Es ist das entsprechende Beantragungsformular auszufüllen: https://www.fernuni-hagen.de/o365gast/creatick
- Externe Personen müssen der Verarbeitung ihrer personenbezogenen Daten und den Nutzungsbedingungen zustimmen.

Einschränkungen

- Es darf kein Zwang zu bestimmtem Verhalten auf die Nutzenden ausgeübt werden. Es wird dringend gebeten, während dienstlicher Teams-Besprechungen die Kamera einzuschalten. Eine Verpflichtung, die Kamera einzuschalten, besteht nicht.

Anlage 2: Verzeichnis der Anwendungen

Applikationen im Einsatz

- Access
- Bookings
- Class Notebook
- Delve
- Excel
- Forms
- Lists
- OneDrive
- OneNote
- Outlook
- Planner
- Power Apps
- Power Automate
- PowerPoint
- Project
- Publisher
- SharePoint
- Staff Notebook
- Stream
- Teams
- ToDo
- Visio
- Whiteboard
- Word
- Yammer

Add-Ons im Einsatz

- FindTime

3rd Party Anwendungen und Schnittstellen, die per Azure SSO angebunden sind

- Backup mit KeepIT
- Citavi AddOn / Assistant
- WebHooks (Schnittstelle)

Anlage 3: Spezifische Regelungen zu Anwendungen und Funktionen von M365

- Der Zugriff auf Microsoft Graph/Delve/Viva ist, soweit in M365 möglich, zu deaktivieren. Sollte eine Deaktivierung nicht möglich sein, ist die Nutzung untersagt.
- Die Einstellungen in der Administration von M365 sind so zu wählen, dass von den verwendeten Geräten der Nutzenden möglichst wenig Telemetriedaten an Microsoft gesendet werden.
- Sofern jeweils technisch möglich werden automatisierte Benachrichtigungen (z.B. über Warnungsrichtlinien) der Personalräte über folgende Aktivitäten im System eingerichtet:
    a. Administratorenzugriffe auf das persönliche Onedrive- bzw. Exchange eines Nutzenden
    b. Start und/oder Export einer e-Discovery
- Die Nutzung von M365-Adminfunktionen (z.B. im Rahmen von e-Discorvery, Globalsuche, Purview, Keywordsuche o.ä. zukünftige Funktionen) bei denen eine Suche innerhalb der persönlichen Daten der Nutzenden stattfindet, bedarf in jedem einzelnen Fall der vorherigen Zustimmung der Personalräte. Sollte auf diese Zustimmung auf Grund von unmittelbaren Sicherheitsgefahren nicht gewartet werden können, so ist im Anschluss die Zustimmung schnellstmöglich einzuholen und die Dringlichkeit der Maßnahme zu begründen.
- Sofern im Rahmen von IT-Sicherheitsmaßnahmen auf persönliche Daten von Nutzenden zugegriffen werden muss, müssen die Betroffenen im Nachgang informiert werden.
- Ein Personenscoring findet nicht statt, die entsprechenden Funktionen sind deaktiviert.

Anlage 4: Schnittstellen in M365 und zu anderen Systemen

Dokumentation personenbezogene Daten und deren Datenflüsse

Schnittstellen, über die Identitäten (Benutzer/Kontakte/Gruppen) in das Azure Active Directory (AD) synchronisiert werden

Azure AD Connect ist eine lokale Microsoft-Anwendung, welche auf einem On-Prem-Server der FernUniversität läuft, der das lokale Active Directory der FernUniversität mit dem Azure AD verbindet.
Azure AD Connect synchronisiert Identitäten (Benutzer/Gruppen/Kontakte) in das Microsoft Azure Active Directory (M365). Weitere Datenzu- oder Datenabflüsse finden nicht statt.

Benutzerobjekte

Nachfolgende Attribute werden bei **Benutzerobjekten** in das Azure Active Directory synchronisiert:

Attribute Name	Beispiel	Erläuterung
accountEnabled	true	true=Account aktiviert false=Account deaktiviert
alias	Mustermann	Benutzername
city	Hagen	Ort, bei jedem Beschäftigten auf Hagen gesetzt
cloudAnchor	*String*	Anker-Attribut zur On-Prem Umgebung
cloudMastered	false	false=Synchronisierter Benutzer aus dem AD On-Prem true= Cloud only Benutzer
commonName	Erika Mustermann (mustermann)	Kombination aus: Vorname, Nachname und Benutzername
company	FernUniversität in Hagen	Organisation, bei jedem Beschäftigten auf FernUniversität in Hagen gesetzt
country	Deutschland	Land, bei jedem Beschäftigten auf Deutschland gesetzt
countryCode	0	Ländercode in

		Binär, bei jedem Beschäftigten auf 0 gesetzt
department	Abteilung	Organisatorische Zuordnung
displayName	Mustermann, Erika	Nachname, Vorname
dnsDomainName	buerokommunikation.fernuni-hagen.de	Domain, unter welcher der Benutzer registriert ist
extensionAttribute1	1	1=Benutzer wird per Azure AD Connect in die Cloud synchronisiert NULL=Benutzer wird nicht synchronisiert
extensionAttribute13	Default	On-Prem Attribut, welches in der Cloud nicht verwendet wird
extensionAttribute14	mailhost	On-Prem Attribut, welches in der Cloud nicht verwendet wird
extensionAttribute15	*String*	On-Prem Attribut, welches in der Cloud nicht verwendet wird
facsimileTelephoneNumber	+49 2331 987 - 123456	Faxnummer
givenName	Erika	Vorname
lastPasswordChangeTimestamp	*Timestamp*	Zeitpunkt des letztes Kennwortwechsel
legacyExchangeDN	*String*	Exchange Steuerungs-Attribut
mail	erika.mustermann@fernuni-hagen.de	E-Mail-Adresse
msExchBlockedSendersHash	*Binary*	Exchange Steuerungs-Attribut
msExchMailboxGuid	*Binary*	Exchange Steuerungs-Attribut
msExchRecipientDisplayType	*Number*	Exchange Steuerungs-Attribut
msExchRecipientTypeDetails	1	Exchange Steuerungs-Attribut
msExchSafeSendersHash	*Binary*	Exchange Steuerungs-Attribut
netBiosName	BUEROKOMMUNIK	Verkürzte Domain, unter welcher der

		Benutzer registriert ist
onPremiseSecurityIdentifier	*Binary*	SecurityIdentifier des AD On-Prem
onPremisesDistinguished-Name	CN=Erika Mustermann (muster-mann),OU=ZMI,OU=IAM-Mana-ged,DC=buerokommunikation,DC=fern-uni-hagen,DC=de	DistinguishedName des AD On-Prem
onPremisesSamAccount-Name	mustermann	SamAccountName des AD On-Prem
physicalDeliveryOfficeName	Geb. 12, 0B123	Gebäude.- und Raumnummer
postOfficeBox	FernUniversität in Hagen	Organisation, bei jedem Beschäftig-ten auf FernUniver-sität in Hagen ge-setzt
postalCode	58097	Postleitzahl, bei je-dem Beschäftigten auf 58084 gesetzt
preferredLanguage	de-DE	Anzeigesprache für M365-Umgebung, bei jedem Beschäf-tigten auf de-DE gesetzt
proxyAddresses	SMTP:erika.mustermann@fernuni-ha-gen.de	Proxy-Adressen
sourceAnchor	*String*	Anker-Attribut zum Azure AD Connect
state	NRW	Bundesland, bei je-dem Beschäftigten auf NRW gesetzt
surname	Mustermann	Nachname
telephoneNumber	+49 2331 987 – 123456	Telefonnummer
thumbnailPhoto		Foto, nur wenn Nutzende dieses selbst hochladen
usageLocation	DE	Standort des Be-nutzers, bei jedem Beschäftigten auf DE gesetzt
userCertificate	*Binary*	Im AD On-Prem hinterletztes Be-nutzer-Zertifikat (z.B. zum ver-schlüsseln Dateien in M365)
userPrincipalName	mustermann@buerokommunikation.fernuni-ha-gen.de	UserPrincipalName des AD On-Prem.

		Diesen verwenden wir als Benutzernamen für M365
userSMIMECertificate	*Binary*	Im AD On-Prem hinterletztes Benutzer-Zertifikat (z.B. zum verschlüsseln von E-Mails über Exchange Online)
manager	vorgesetzte Person	Organisatorischer Vorgesetzter
unicodePwd-Attribut	*Hashwert des Kennworts*	Hashwert des Kennworts. Weitere Informationen zum Mechanismus: https://learn.microsoft.com/de-de/azure/active-directory/hybrid/connect/how-to-connect-password-hash-synchronization

Gruppenobjekte

Nachfolgende Attribute werden bei **Gruppenobjekten** in das Azure Active Directory synchronisiert:

Attribute Name	**Beispiel**	**Erläuterung**
cloudAnchor	*String*	Anker-Attribut zur On-Prem Umgebung
cloudMastered	False	false=Synchronisierter Benutzer aus dem AD On-Prem true= Cloud only Benutzer
commonName	G-MIM_AllUsers	Name der AD-Gruppe
displayName	G-MIM_AllUsers	Name der AD-Gruppe
dnsDomainName	buerokommunikation.fernuni-hagen.de	Domain, unter welcher die Gruppe registriert ist
extensionAttribute1	1	1=Gruppe wird per Azure AD Connect in die Cloud synchronisiert NULL=Gruppe wird nicht synchronisiert
netBiosName	BUEROKOMMUNIK	Verkürzte Domain, unter welcher die Gruppe registriert ist
onPremiseSecurityIdentifier	*Binary*	SecurityIdentifier des AD On-Prem
onPremisesSamAccountName	G-MIM_AllUsers	SamAccountName des AD On-Prem
securityEnabled,boolean,true	True	true=Sicherheitsgruppe false=Keine

		Sicherheitsgruppe
sourceAnchor	*String*	Anker-Attribut zum Azure AD Connect

Kontaktobjekte

Kontaktobjekte werden an der FernUniversität nicht genutzt und daher nicht über Azure AD Connect in die Microsoft Cloud synchronisiert.

Weitere Informationen zu den Attributen

https://learn.microsoft.com/de-de/azure/active-directory/hybrid/connect/reference-connect-sync-attributes-synchronized

Schnittstelle zu Keepit

Keepit ist der Backup-Service folgender Microsoft-Anwendungen:

- exchange online-backup
- onedrive-backup
- sharepoint- und teams-backup

Anlage 5: Rollen und Berechtigungskonzept

Administratorrolle	**Wem sollte diese Rolle zugewiesen werden?**	Orga-Bereich
Abrechnungsadministrator	Weisen Sie die Rolle des Abrechnungsadministrators Benutzern zu, die Einkäufe tätigen, Abonnements und Dienstanforderungen verwalten und den Dienststatus überwachen. Abrechnungsadministratoren können ebenfalls: – Alle Aspekte der Abrechnung verwalten – Supporttickets im Azure-Portal erstellen und verwalten	ZDI, KompetenzCentrum Rechenzentrum
Exchange-Administrator	Weisen Sie die Exchange-Administratorrolle Benutzern zu, die die E-Mail-Postfächer Ihrer Benutzer, Microsoft 365-Gruppen und Exchange Online einsehen und verwalten müssen. Exchange-Administratoren sind außerdem zu Folgendem berechtigt: - Wiederherstellen gelöschter Elemente im Postfach eines Benutzers - Einrichten von "Senden als"- und "Senden im Auftrag von"-Stellvertretungen	ZDI, KompetenzCentrum Webportal-/Serveranwendungen
Globaler Administrator	Weisen Sie Benutzern, die globalen Zugriff auf die meisten Verwaltungsfunktionen und Daten in Microsoft Online-Diensten benötigen, die Rolle des globalen Administrators zu. Wenn Sie zu vielen Benutzern globalen Zugriff gewähren, besteht ein Sicherheitsrisiko, deshalb empfiehlt es sich, nur zwei bis vier globale Administratoren vorzusehen. Nur globale Administratoren sind zu Folgendem berechtigt: - Zurücksetzen von Kennwörtern für alle Benutzer - Hinzufügen und Verwalten von Domänen **Hinweis:** Die Person, die die Registrierung für Microsoft-Onlinedienste vorgenommen hat, wird automatisch zu einem globalen Administrator.	GlobAdminProd: Personifizierte Funktions-Account () Extern: Hansevision
Globaler Leser	Weisen Sie die Rolle „Globaler Leser“ Benutzern zu, die Administratorfeatures und -einstellungen in Admin Centern anzeigen müssen, die der globale Administrator anzeigen kann. Der „Globaler	ZDI, Kompetenz-Centrum Rechenzentrum

	Leser"-Administrator kann keine Einstellungen bearbeiten.	
Gruppenadministrator	Weisen Sie die Rolle des Gruppenadministrators Benutzern zu, die alle Gruppeneinstellungen in den Admin Centern verwalten müssen, einschließlich des Microsoft 365 Admin Centers und des Azure Active Directory-Portals. Gruppenadministratoren sind zu Folgendem berechtigt: - Erstellen, Bearbeiten, Löschen und Wiederherstellen von Microsoft 365-Gruppen - Einrichten und Aktualisieren von Erstellung, Ablauf und Benennungsrichtlinien von bzw. für Gruppen - Erstellen, Bearbeiten, Löschen und Wiederherstellen von Azure Active Directory-Sicherheitsgruppen	(werden aktuell nicht benötigt)
Helpdesk-Administrator	Weisen Sie die Rolle des Helpdesk-Administrators Benutzern zu, die folgende Aktionen ausführen müssen: - Kennwörter zurücksetzen - Die Abmeldung von Benutzern erzwingen - Serviceanfragen verwalten - Den Dienststatus überwachen **Hinweis**: Der Helpdesk-Administrator kann nur Benutzern ohne Administratorrolle sowie Benutzern helfen, welchen folgende Rollen zugewiesen wurden: Verzeichnisleseberechtigter, Gasteinladender, Helpdesk-Administrator, Nachrichtencenter-Leseberechtigter und Berichtleseberechtigter.	ZDI, Kompetenz-Centrum Rechenzentrum
Lizenzadministrator	Weisen Sie die Rolle des Lizenzadministrators Benutzern zu, die Lizenzen für Benutzer zuweisen und entfernen und deren Verwendungsort bearbeiten müssen. Lizenzadministratoren können ebenfalls: – Lizenzzuweisungen für die gruppenbasierte Lizenzierung erneut verarbeiten – Produktlizenzen für die gruppenbasierte Lizenzierung an Gruppen zuweisen	ZDI, Kompetenz-Centrum Rechenzentrum
Administrator für Office-Apps	Weisen Sie die Rolle des Office-Apps-Administrators Benutzern zu, die folgende Aktionen ausführen müssen: - Verwenden des Office-Cloudrichtliniendiensts zum Erstellen und Verwalten von cloudbasierten Richtlinien für Office - Serviceanfragen erstellen und verwalten - Verwalten der Inhalte im Dialogfenster	Nicht in Benutzung

	"Neuigkeiten", das den Benutzern in ihren Office-Apps angezeigt wird - Den Dienststatus überwachen	
Kennwortadministrator	Weisen Sie die Rolle des Kennwortadministrators Benutzern zu, die Kennwörter für Nicht-Administratoren und Kennwortadministratoren zurücksetzen müssen.	(Kennwörter über AD zurückgesetzt)
Nachrichtencenter-Lesebe-rechtigter	Weisen Sie die Rolle „Nachrichtencenter-Lesebe-rechtigter“ Benutzern zu, die Folgendes ausführen müssen: – Überwachen der Nachrichtencenter-Benachrichtigungen – Wöchentliche E-Mail-Zusammenfassungen von Beiträgen und Aktualisierungen des Nachrichtencenters erhalten – Freigeben von Beiträgen im Nachrichtencenter – Schreibgeschützten Zugriff auf Azure AD-Dienste haben, wie z. B. Benutzer und Gruppen	(Alle 365 Administratoren)
Power Plattform-Administrator	Weisen Sie die Power Plattform-Administratorrolle Benutzern zu, die Folgendes ausführen müssen: – Verwalten aller Administratorfunktionen für Power Apps, Power Automate und die Verhinderung von Datenverlust – Serviceanfragen erstellen und verwalten – Den Dienststatus überwachen	Nicht in Benutzung
Berichtleseberechtigter	Weisen Sie die Rolle „Berichtleseberechtigter“ Benutzern zu, die folgende Aktionen ausführen müssen: – Nutzungsdaten und Aktivitätsberichte im Microsoft 365 Admin Center anzeigen – Zugriff auf das Inhaltspakets zur Power BI-Einführung erhalten – Zugriff auf Anmeldeberichte und Aktivitäten in Azure AD erhalten – Vom Microsoft Graph-Berichterstellungs--API zurückgegebene Daten anzeigen	ZDI, Kompetenz-Centrum Rechenzentrum
Dienstsupportadministrator	Weisen Sie die Rolle des Dienstsupportadministrators als zusätzliche Rolle Administratoren oder Benutzern zu, die zusätzlich zu ihrer normalen Administratorrolle folgende Aufgaben erfüllen müssen: - Serviceanfragen öffnen und verwalten - Nachrichtencenter-Beiträge anzeigen und freigeben - Den Dienststatus überwachen	ZDI, Kompetenz-Centrum Rechenzentrum
SharePoint-Administrator	Weisen Sie die SharePoint-Administratorrolle Benutzern zu, die auf das SharePoint Online Admin Center zugreifen und dieses verwalten müssen.	ZDI, Kompetenzcentrum Rechenzentrum, Infrastruktur

	Wir unterscheiden zwischen Administrativen (one drive) und Inhaltlichen Themen (online) Die Benutzerrechte sind in dem Fall aber identisch. SharePoint-Administratoren sind zudem zu Folgendem berechtigt: - Erstellen und Löschen von Websites - Verwalten von Websitesammlungen - Verwalten von globalen SharePoint-Einstellungen	svc-automate ==> Funktions-Account svc-migrate ==> Funktions-Account
Teams-Administrator	Weisen Sie die Teams-Administratorrolle Benutzern zu, die auf das Teams Admin Center zugreifen und dieses verwalten müssen. Der Teams-Administrator kann auch folgende Aktionen ausführen: - Verwalten von Besprechungen - Verwalten von Konferenzbrücken - Verwalten aller organisationsweiten Einstellungen einschließlich Partnerverbund, Microsoft Teams-Upgrades und Einstellungen des Microsoft Teams-Clients	ZDI, Kompetenz-Centrum Rechenzentrum
Benutzeradministrator	Weisen Sie die Rolle des Benutzeradministrators Benutzern zu, die folgende Aktionen für alle Benutzer ausführen müssen: - Benutzer und Gruppen hinzufügen - Lizenzen zuweisen - Die meisten Benutzereigenschaften verwalten - Benutzeransichten erstellen und verwalten - Kennwortablaufrichtlinien aktualisieren - Serviceanfragen verwalten - Den Dienststatus überwachen Der Benutzeradministrator kann außerdem die unten aufgeführten Aktionen für Benutzer ohne Administratorrolle sowie für Benutzer ausführen, denen die folgenden Rollen zugewiesen sind: Verzeichnisleseberechtigter, Gasteinladender, Helpdesk-Administrator, Nachrichtencenter-Leseberechtigter und Berichtleseberechtigter. - Benutzernamen verwalten - Benutzerkonten löschen und wiederherstellen - Kennwörter zurücksetzen - Die Abmeldung von Benutzern erzwingen - (FIDO)-Geräteschlüssel aktualisieren	ZDI, Kompetenz-Centrum Rechenzentrum svc-migrate ==> Funktions-Account

Bei Bedarf können die Interessenvertretungen die namentliche Zuordnung zu den jeweiligen Administratorenrollen einsehen.

Anlage 6: Lösch- und Sperrkonzept

1. Die persönlichen Speicherorte der Nutzenden in M365 (Exchange-Postfach, Sharepoint, Chatverläufe, pers. Onedrive, usw.) sind, mit Ausnahme der von den Nutzenden selbst initiierten Teilen- und Freigabefunktionen grundsätzlich für niemanden einsehbar und vor Zugriffen anderer Personen technisch zu schützen.
2. Alle Ausnahmen von dieser grundsätzlichen Regel werden in dieser Dienstvereinbarung inklusive der Anlagen abschließend geregelt:
   a. Sollte nach dem Ausscheiden des Nutzenden aus der FernUniversität die Notwendigkeit eines Zugriffs auf persönliche Speicherorte bestehen, so kann dies in Ausnahmefällen nach Zustimmung des zuständigen Personalrats und unter Aufsicht des Personalrats und Datenschutzbeauftragten geschehen.
   b. Sollten es besondere dringende Umstände (z.B. längerfristiger Nichterreichbarkeit eines Nutzenden) erforderlich machen, auf die persönlichen Speicherorte eines Nutzenden zuzugreifen, so kann dies nach Zustimmung des zuständigen Personalrats und unter Aufsicht des Personalrats und Datenschutzbeauftragten geschehen.
3. Der Microsoft 365 Account eines Beschäftigten wird, vorbehaltlich Absatz 4, am Tag des Austritts (Ende des Beschäftigungsverhältnisses) deaktiviert, sodass ein Zugriff auf die Daten nicht mehr möglich ist.
4. Die Daten in den persönlichen Speicherorten bleiben 30 Tage nach Ausscheiden aus der FernUniversität gespeichert. Nach Ablauf der Frist erfolgt eine automatische Löschung.
5. Vorgesetzte und Beschäftigte haben vor Ausscheiden aus der FernUniversität eine geordnete Übergabe zu organisieren. 20 Tage vor Ausscheiden erfolgt dazu eine automatische Erinnerung an Vorgesetzte und Beschäftigte.

Anlage 7: Verzeichnis Dienstleistende zum Betrieb, Service oder Wartung

Dienstleistende der FernUniversität:

Bechtle GmbH / Hansevision
Walther-Bruch-Str. 9
44263 Dortmund
Zweck: Support- und Betriebsunterstützung der techn. Plattform Microsoft 365

Oxford Computer Group GmbH
Gießereistr. 16
85435 Erding
Zweck: Support- und Betriebsunterstützung Identity-Management-System

Keepit HG
Per Henrik Lings Allé 4, 7th
2100 København
Dänemark
Zweck: Cloud-Backup

Microsoft Deutschland GmbH
Walter-Gropius-Straße 5
80807 München

Dienstleistende/Auftragsdatenverarbeitung für Microsoft:
Link: https://go.microsoft.com/fwlink/?linkid=2096306