

Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto

Microsoft 365 · Hochschule · Identität

Identity Lifecycle an der Hochschule: Von der Immatrikulation bis zum Alumni-Konto

Tausende Konten rein, tausende raus, zweimal im Jahr. Wer das von Hand macht, macht es nicht lange.



boddenberg.de

WISSEN

Alle Beiträge der Serie zu Microsoft 365 in Hochschule und Forschung an einem Ort.

› [Microsoft 365 in Hochschule und Forschung](#)

BERATUNG

Identity Lifecycle entwerfen: Quellsysteme, Rollenlogik, Fristen und Lizenzgruppen, bevor der nächste Semesterstart kommt.

› [Beratung für Hochschulen und Forschung](#)

SCHULUNG

Für Rechenzentrum und Fakultäts-IT: Entra ID, Synchronisation und gruppenbasierte Lizenzen im Hochschulbetrieb.

› [Schulungen für Hochschulen und Forschung](#)

Jedes Hochschulrechenzentrum kennt die zwei Wochen im Jahr, in denen niemand Urlaub nimmt. Kurz vor Vorlesungsbeginn kommen die Neuen, und zwar nicht einzeln, sondern als Jahrgang: ein paar tausend Studenten an einer mittelgroßen Universität, ein paar hundert an einer Kunsthochschule, dazu Doktoranden, neue wissenschaftliche Mitarbeiterinnen und Mitarbeiter, studentische Hilfskräfte mit frisch unterschriebenem Vertrag und Lehrbeauftragte, die ihren Lehrauftrag drei Tage vor der ersten Sitzung erhalten haben. Alle wollen am ersten Tag ins WLAN, ins LMS, ins Postfach und in Teams. Und auf der anderen Seite der Rechnung verlassen fast genauso viele Menschen die Hochschule, nur deutlich leiser.

Identity Management an der Hochschule ist deshalb vor allem ein Durchsatzproblem. Die einzelne Kontoanlage ist trivial. Schwierig wird es, wenn zehntausende Konten pro Jahr kommen, die Rolle wechseln und wieder gehen sollen, und zwar zuverlässig, nachvollziehbar und ohne dass ein Mensch dafür die Maus bewegt. Mit Microsoft 365 und Entra ID kommt ein weiteres Ziel in die Kette, und mit ihm eine neue Ressource, die man verlieren kann: die Lizenz.

Dieser Beitrag geht die Lebenslinie eines Kontos von der Immatrikulation bis zur Frage nach dem Alumni-Konto durch. Er erklärt die Kette aus Quellsystemen, Identity-Management-System, Active Directory, Synchronisation nach Entra ID und gruppenbasierter Lizenzzuweisung, zeigt, wie man Doppelrollen ohne Doppelkonto abbildet, und klärt, was bei der Exmatrikulation mit Postfach, OneDrive und Teams-Mitgliedschaften geschieht. Er gehört zur Serie [Microsoft 365 in Hochschule und Forschung](#). Universitätsklinika und allgemeinbildende Schulen haben eigene Regeln und sind hier nicht gemeint.

FAKTEN · Worum es in diesem Beitrag geht

Quellsysteme: Campus-Management für Studenten, Personalsystem für das Personal, eine geordnete Erfassung für Sonderrollen.

Kette: Identity-Management-System, Active Directory, Synchronisation nach Entra ID, gruppenbasierte Lizenzen.

Doppelrollen: Student und studentische Hilfskraft, Doktorand und Mitarbeiter, jeweils mit einem einzigen Konto.

Austritt: Karenzzeit, Postfach, OneDrive, Teams und die Alumni-Frage.

Das Problem heißt Durchsatz, nicht Technik

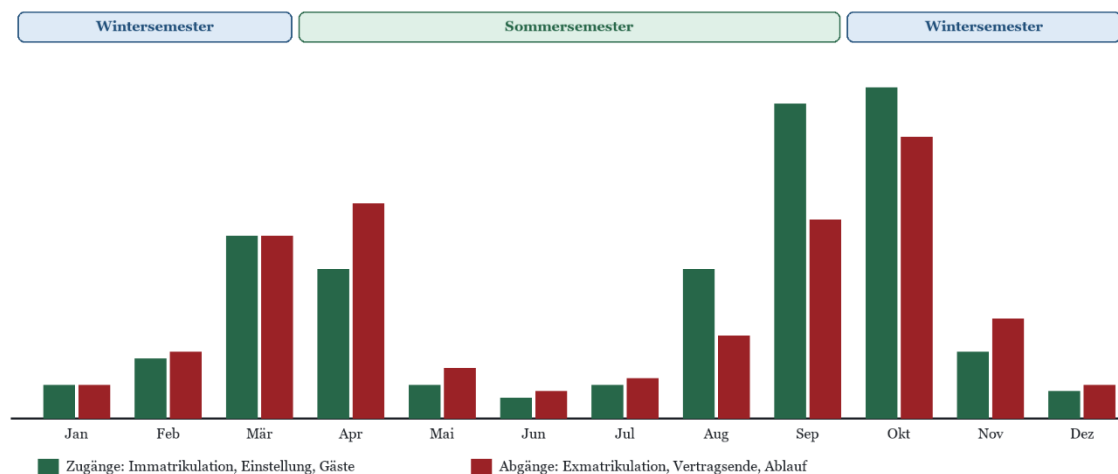
In einem Unternehmen mit fünftausend Mitarbeitern wechseln im Jahr vielleicht einige hundert Personen. Die Personalabteilung meldet jeden Eintritt einzeln, und wenn das Konto einen Tag zu spät kommt, sitzt der neue Kollege eben einen Tag mit dem Handbuch da. An einer Hochschule mit zwanzigtausend Studenten wird im Schnitt in jedem Studienjahr ein erheblicher Teil der Studentenschaft ausgetauscht. Dazu kommen befristete Verträge im wissenschaftlichen Bereich, die eher die Regel als die Ausnahme sind, Hilfskraftverträge über ein Semester und Gäste, die für drei Monate an einem Institut forschen.

Zwei Wellen pro Jahr

Die Bewegungen verteilen sich nicht gleichmäßig. Zum Wintersemester kommt die große Welle, zum Sommersemester die kleinere, und die Exmatrikulationen ballen sich nach Ende der Rückmeldefrist und nach den Prüfungszeiträumen. Wann genau, hängt von Hochschultyp, Bundesland und Prüfungsordnung ab; das Muster ist überall gleich. Skizze 1 zeigt den Verlauf schematisch.

Skizze 1: Das Jahr eines Hochschulrechenzentrums in Kontenbewegungen

Schematisch, ohne Zahlen: Zugänge und Abgänge ballen sich um die Semester Grenzen. Dazwischen ist es ruhig, aber nie still.



Die Spitzen liegen genau dort, wo auch Rückmeldung, Prüfungsanmeldung und Vorlesungsbeginn den Helpdesk fluten.

Schematische Darstellung. Verlauf und Ausprägung unterscheiden sich je nach Hochschultyp und Bundesland.

Die Spitzen liegen leider nicht zufällig dort, wo ohnehin alles brennt. Wer zum Semesterstart Konten anlegt, kämpft gleichzeitig mit der Rückmeldung, der Prüfungsanmeldung, neuen Kursen im LMS und einem Helpdesk, das vor lauter Kennwortrücksetzungen nicht zum Atmen kommt. Jeder Prozess, der in dieser Zeit eine Handarbeit voraussetzt, wird zum Engpass. Und jeder

Engpass wird zu einer Schlange vor dem Servicezentrum, deren Länge man in Semesterwochen messen kann.

Warum die Hochschule kein Unternehmen ist

Drei Eigenheiten machen den Hochschulfall härter als den Normalfall, für den Microsoft seine Dokumentation schreibt. Erstens gibt es mindestens zwei führende Quellsysteme, die nichts voneinander wissen: das Campus-Management für die Studenten und das Personalsystem für Professoren, Mitarbeiterinnen und Mitarbeiter. Zweitens sind Rollen nicht exklusiv. Ein Mensch kann gleichzeitig Student, Hilfskraft am Lehrstuhl und Mitglied einer Gremienkommission sein. Drittens kommen Menschen wieder: Nach dem Bachelor folgt der Master, nach dem Master die Promotion, nach dem Vertragsende der nächste Drittmittelvertrag.

Dazu kommt das Organisatorische. Die Hochschulverwaltung verantwortet die Quelldaten, das Rechenzentrum die Technik, die Fakultäten verwalten oft eigene Gruppen und manchmal eigene Systeme. Wie man das mit einem gemeinsamen Tenant zusammenbringt, beschreibt [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#). Für den Lebenszyklus gilt: Ohne klare Zuständigkeit für jedes Attribut gibt es keinen sauberen Lebenszyklus.

WARNUNG · Wer Lizenzen von Hand zuweist, verliert zum Semesterstart

Die Rechnung ist einfach. Wenn zum Wintersemester mehrere tausend Konten in wenigen Tagen entstehen und jedes einzeln im Admin Center eine Lizenz bekommt, fehlt irgendwo eine. Dann hat ein Erstsemester kein Postfach, ein anderer zwei Lizenzen, und die Exmatrikulierten des letzten Jahres belegen noch immer Lizenzen, die niemand zurückgeholt hat.

Handzuweisungen haben außerdem kein Gedächtnis. Niemand weiß im Nachhinein, warum ein Konto eine bestimmte Lizenz trägt. Bei der nächsten Lizenzzählung, beim nächsten Audit und beim nächsten Wechsel des Lizenzmodells steht das Rechenzentrum dann mit einer Excel-Liste und viel Hoffnung da.

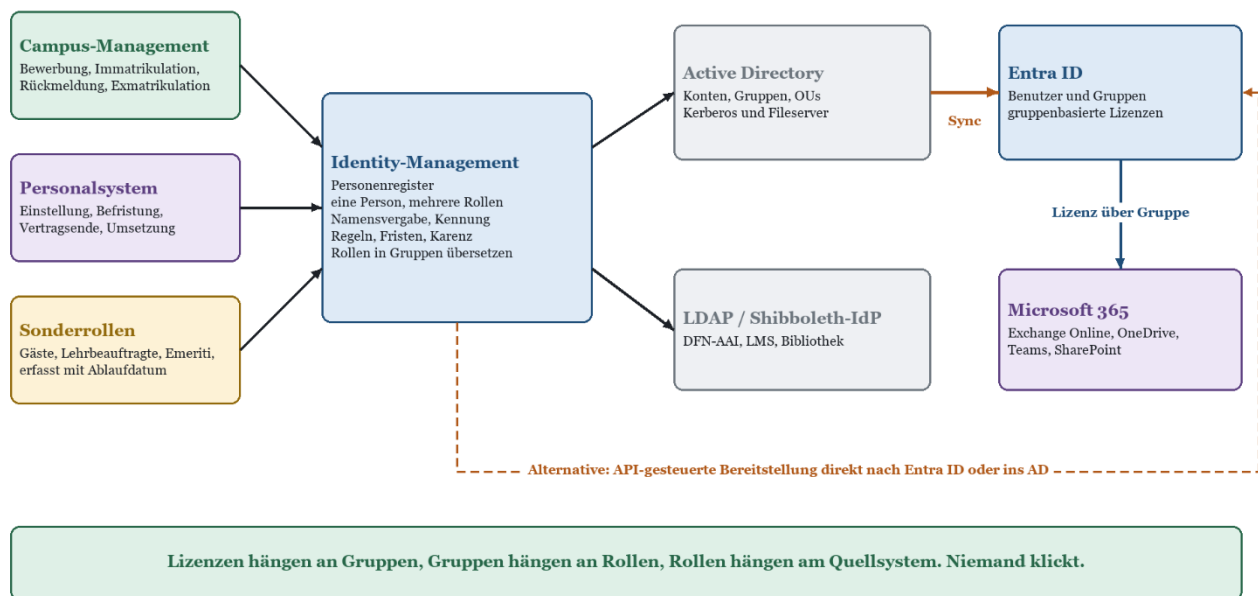
Die Regel lautet deshalb: Lizenzen hängen an Gruppen, Gruppen hängen an Rollen, Rollen kommen aus dem Quellsystem. Direkte Zuweisungen sind die dokumentierte Ausnahme, nicht der Arbeitsalltag.

Die Kette: Quellsystem, Identity-Management, Active Directory, Entra ID

Ein belastbarer Identity Lifecycle an der Hochschule hat vier Stufen. Jede Stufe hat eine Aufgabe, und keine Stufe sollte die Aufgabe einer anderen übernehmen. Skizze 2 zeigt die Kette im Überblick.

Skizze 2: Die Kette vom Quellsystem bis zur Lizenz

Jede Stufe hat genau eine Aufgabe. Wer eine Stufe überspringt, baut sich einen zweiten Wahrheitsbegriff ein.



Schematische Darstellung. Ob LDAP und AD getrennt sind und welches IdM-Produkt im Einsatz ist, unterscheidet sich je Hochschule.

Quellsysteme: Wer ist führend?

Für Studenten ist das Campus-Management führend. Dort entstehen Bewerbung, Zulassung, Immatrikulation, Rückmeldung, Beurlaubung, Fachwechsel und Exmatrikulation, jeweils mit Datum. Für das Personal ist es das Personalsystem mit Einstellung, Befristung, Umsetzung und Vertragsende. Für alle, die in keinem dieser beiden Systeme stehen, also Gastwissenschaftler, Lehrbeauftragte ohne Vertrag im Personalsystem, Emeriti, Stipendiaten oder Mitarbeiter von An-Instituten, braucht es eine dritte, geordnete Erfassung mit Antragsteller, verantwortlicher Person und Ablaufdatum.

Führend heißt: Das Quellsystem entscheidet, ob es eine Person in einer Rolle gibt und ab wann nicht mehr. Das Rechenzentrum entscheidet nicht darüber, ob jemand Student ist. Es entscheidet darüber, was aus dieser Tatsache technisch folgt. Diese Trennung klingt banal, rettet aber in der Diskussion mit dem Prüfungsamt oder dem Personaldezernat regelmäßig den Nachmittag.

Das Identity-Management als Personenregister

Das Identity-Management-System ist an den meisten Hochschulen längst vorhanden, oft als Eigenentwicklung, die seit Jahren gewachsen ist, manchmal als kommerzielles oder quelloffenes Produkt. Für Microsoft 365 muss es nicht ersetzt werden, und in aller Regel sollte es das auch nicht. Seine Aufgaben bleiben dieselben: Personen aus mehreren Quellen zusammenführen, Dubletten erkennen, eine dauerhafte Kennung vergeben, Rollen und Fristen verwalten und daraus Konten und Gruppen in den Zielsystemen ableiten.

Entscheidend ist die dauerhafte Kennung. Sie ist das Bindeglied zwischen dem Menschen und allem, was in Microsoft 365 an seinem Konto hängt: Postfach, OneDrive, Teams-Mitgliedschaften, MFA-Registrierung. Ändert sich die Kennung, weil jemand vom Bachelor in den Master wechselt und eine neue Matrikelnummer bekommt, entsteht im schlimmsten Fall ein neues Konto mit leerem OneDrive. Die Matrikelnummer ist deshalb ein Attribut, aber kein guter Schlüssel.

Active Directory und Synchronisation nach Entra ID

Die meisten Hochschulen betreiben ein Active Directory, weil Fileserver, Poolrechner, Druckdienste und Kerberos daran hängen. Dann ist der übliche Weg: Das IdM schreibt Konten und Gruppen ins AD, und Entra Connect oder Entra Cloud Sync synchronisiert sie nach Entra ID. Wer kein AD für Studenten betreibt oder es abbauen möchte, kann Konten auch ohne Umweg in Entra ID anlegen, etwa über die API-gesteuerte eingehende Bereitstellung von Entra ID oder direkt über Microsoft Graph aus dem IdM heraus.

Weg	Wie er funktioniert	Stärken	Worauf achten
Entra Connect	Synchronisation aus dem lokalen AD nach Entra ID, Server im eigenen Haus	ausgereift, viele Filter- und Regelmöglichkeiten, Hybrid-Exchange-tauglich	eigener Server mit Pflegeaufwand; Regeländerungen brauchen Erfahrung
Entra Cloud Sync	leichter Agent im AD, Konfiguration in der Cloud	einfacher Betrieb, mehrere Agenten für Ausfallsicherheit	Funktionsumfang vor der Entscheidung gegen die eigenen Anforderungen prüfen
API-gesteuerte eingehende Bereitstellung	IdM oder Skript sendet Personendaten an eine Graph-Schnittstelle, Entra legt Konten im AD oder in Entra ID an	keine eigene Abgleichslogik nötig, Protokolle in Entra	Tageskontingent an Aufrufen, setzt Entra ID P1 oder höher voraus
IdM direkt über Microsoft Graph	IdM legt Konten und Gruppen selbst in Entra ID an	volle Kontrolle im eigenen System	Abgleich, Fehlerbehandlung und Drosselung liegen komplett beim IdM

FAKTEN · API-gesteuerte Bereitstellung im Semesterstart

Microsoft beschreibt für die API-gesteuerte eingehende Bereitstellung zwei Grenzen: höchstens 40 Aufrufe in einem Fünf-Sekunden-Fenster und ein Tageskontingent pro Tenant, das mit Entra ID P1 oder P2 bei 2.000 Aufrufen und mit Entra ID Governance bei 6.000 Aufrufen liegt. Ein Aufruf soll bis zu 50 Operationen bündeln.

Rechnerisch sind das mit P1 bis zu 100.000 Benutzeroperationen am Tag. Das reicht für einen Semesterstart, aber nicht für einen naiven Vollabgleich, der jede Nacht alle Personen einzeln schickt und nebenbei noch Fehler wiederholt. Planen Sie Delta-Übertragungen und Bündelung von Anfang an ein.

Gruppenbasierte Lizenzzuweisung

Am Ende der Kette steht die Lizenz. Entra ID kann Lizenzen an Gruppen hängen: Wer Mitglied ist, bekommt die Lizenz, wer die Gruppe verlässt, verliert sie. Microsoft setzt dafür Entra ID P1 oder einen Office-365-Plan ab A3 voraus. Die Gruppen können aus dem AD synchronisiert sein oder in Entra ID dynamisch über Attribute gebildet werden, etwa über ein Attribut, das die aktive Rolle trägt. Verschachtelte Gruppen wertet die Lizenzzuweisung nicht aus; nur direkte Mitglieder bekommen eine Lizenz.

Für die Hochschule bewährt sich ein kleines, stabiles Set an Lizenzgruppen: eine Gruppe für Studenten, eine für Personal, gegebenenfalls eine für Sonderrollen und eine für Konten, die bewusst ohne Lizenz bleiben. Welche Education-Pläne hinter diesen Gruppen stehen und wie die Studentenzulizenzen mit den Personallizenzen zusammenhängen, beschreibt [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#). Hier geht es nur um die Mechanik.

Drei Fallen sollten Sie kennen. Erstens verlangt jede Lizenz einen Nutzungsstandort am Konto; fehlt er, erbt das Konto bei gruppenbasierter Zuweisung den Standort des Tenants, was für eine deutsche Hochschule meist passt, für internationale Außenstellen aber nicht immer. Zweitens zeigt das Admin Center Fehler wie fehlende Lizenzen oder widersprüchliche Dienstpläne gesammelt an, aber nur wer dort regelmäßig nachsieht, bemerkt sie. Drittens verarbeitet Microsoft Lizenzänderungen für sehr große Gruppen in Lastspitzen nicht sofort; zum Semesterstart sollten Sie also nicht davon ausgehen, dass eine Lizenz Sekunden nach dem Gruppenbeitritt wirkt.

TIPP · Erst in die neue Gruppe, dann aus der alten

Wechselt jemand von einer Lizenzgruppe in eine andere, etwa vom Studenten zum wissenschaftlichen Mitarbeiter, empfiehlt Microsoft eine feste Reihenfolge: zuerst in die Zielgruppe aufnehmen, prüfen, dass die neue Lizenz angekommen ist, dann aus der alten Gruppe entfernen. Umgekehrt ist das Konto für die Dauer der Verarbeitung ohne Lizenz, und in großen Tenants kann diese Dauer länger sein, als einem lieb ist. Bauen Sie diese Reihenfolge direkt in die IdM-Regeln ein.

Doppelrollen: Eine Person, ein Konto

Die häufigste Sünde im Hochschul-Tenant ist das Zweitkonto. Es entsteht ganz harmlos: Der Student hat sein Konto aus dem Campus-Management, dann unterschreibt er einen Hilfskraftvertrag, und das Personalsystem meldet einen neuen Mitarbeiter. Das IdM erkennt die Person nicht wieder, oder es gibt gar kein IdM, das beide Quellen kennt, und schon gibt es zwei Konten, zwei Postfächer, zwei OneDrives und zwei MFA-Registrierungen. Nach zwei Jahren weiß niemand mehr, in welchem Konto die Daten des Lehrstuhls liegen. Spätestens beim Vertragsende wird es dann spannend.

Typische Kombinationen

Kombination	Quellen	Führende Rolle für Lizenz und Adresse	Besonderheit
Student und studentische Hilfskraft	Campus-Management, Personalsystem	in der Regel Personal, solange der Vertrag läuft	Vertragsende mitten im Studium: zurück zur Studentenlizenz, Daten des Lehrstuhls vorher übergeben
Doktorand und wissenschaftlicher Mitarbeiter	Promotionsverwaltung oder Campus-Management, Personalsystem	Personal	Vertrag endet oft vor der Promotion; Konto muss als Doktorand weiterleben
Doktorand ohne Vertrag	Promotionsverwaltung oder Campus-Management	je nach Hochschulregelung Student oder Sonderrolle	Stipendiaten und externe Doktoranden fallen leicht durchs Raster
Mitarbeiter, der ein Studium beginnt	Personalsystem, Campus-Management	Personal	Studienrolle bringt Kursgruppen mit, ändert aber nicht die dienstliche Adresse
Professor mit Lehrauftrag an einer zweiten Hochschule	nur das eigene Personalsystem	Personal an der Heimathochschule	an der zweiten Hochschule eher Gast als zweites Mitgliedskonto

Lizenz, Adresse und Gruppen

Damit eine Person mit mehreren Rollen ein einziges Konto behält, braucht das IdM drei Regeln. Die erste regelt die Lizenz: Wer eine aktive Personalrolle hat, landet in der Personal-Lizenzgruppe

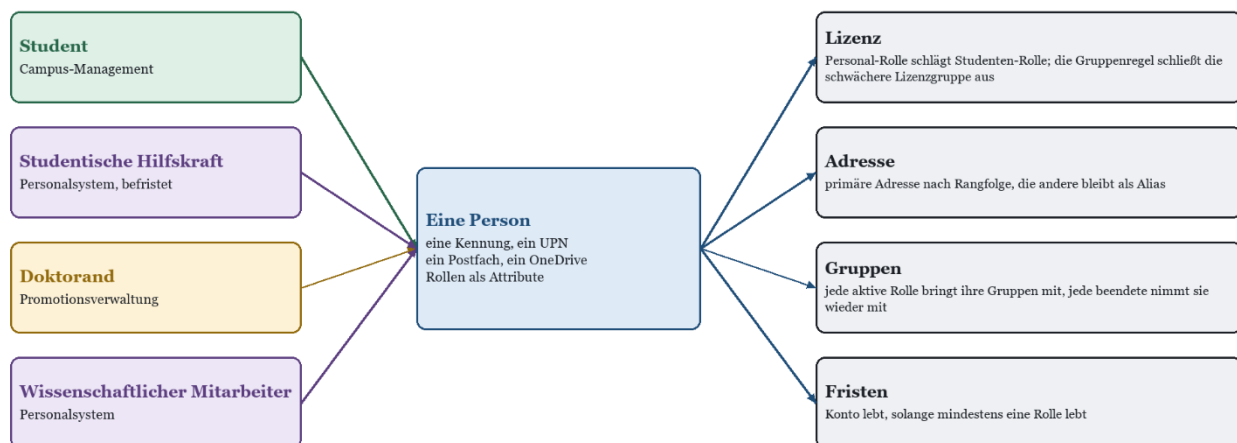
und wird aus der Studenten-Lizenzgruppe ausgeschlossen. Bei dynamischen Gruppen in Entra ID heißt das konkret, dass die Regel für Studenten eine aktive Personalrolle ausdrücklich ausschließt. Sonst sammelt das Konto beide Lizenzen ein, und das fällt erst bei der nächsten Lizenzzahlung auf.

Die zweite Regel betrifft die Adresse. Viele Hochschulen trennen die Studentendomäne von der Personaldomäne. Bei einer Doppelrolle bestimmt eine Rangfolge, welche Adresse primär ist; die andere bleibt als zusätzliche Adresse erhalten, damit Post nicht verloren geht. Ändert sich die primäre Adresse, ändert sich oft auch der Anmeldename. Ob der Anmeldename deshalb rollenneutral sein sollte, ist eine der wichtigsten Grundsatzentscheidungen des ganzen Vorhabens; wer sie früh trifft, erspart sich später sehr viele Umbenennungen.

Die dritte Regel betrifft die Gruppen. Jede aktive Rolle bringt ihre Gruppen mit: der Studiengang die Kursgruppen, der Hilfskraftvertrag die Lehrstuhlgruppe. Endet die Rolle, nimmt sie ihre Gruppen wieder mit. Das Konto selbst lebt, solange mindestens eine Rolle lebt. Skizze 3 fasst das zusammen.

Skizze 3: Doppelrollen ohne Doppelkonto

Die Rollen kommen aus verschiedenen Quellsystemen, das Konto bleibt eines. Die Logik dazwischen entscheidet über Lizenz, Adresse und Gruppen.



Anti-Pattern: das Zweitkonto

- Zwei OneDrives, zwei Postfächer, zwei MFA-Registrierungen.
- Zwei Lizenzen, von denen eine niemand gezählt hat.
- Und am Ende der Hilfskraftzeit die Frage, welches Konto die Daten des Lehrstuhls hatte.

Schematische Darstellung. Rangfolge und Regeln sind eine Entscheidung der Hochschule, keine Produkteigenschaft.

TYPISCHE SITUATION · Ein Mensch, zwei Verträge

Aus Projekten bei öffentlichen Auftraggebern kennen wir das Muster gut. In einem Krankenhausverbund hatten Mitarbeiter, die neben ihrer Stelle in der Pflege auch Lehraufgaben an der angeschlossenen Schule übernahmen, über Jahre zwei Konten, weil zwei Personalbereiche getrennt meldeten. Bei einer Stadtverwaltung war es die Kombination aus Verwaltungsstelle und Ehrenamt bei der Feuerwehr. In beiden Fällen ließ sich das Problem nicht im Verzeichnis lösen, sondern nur dort, wo die Personen zusammengeführt werden.

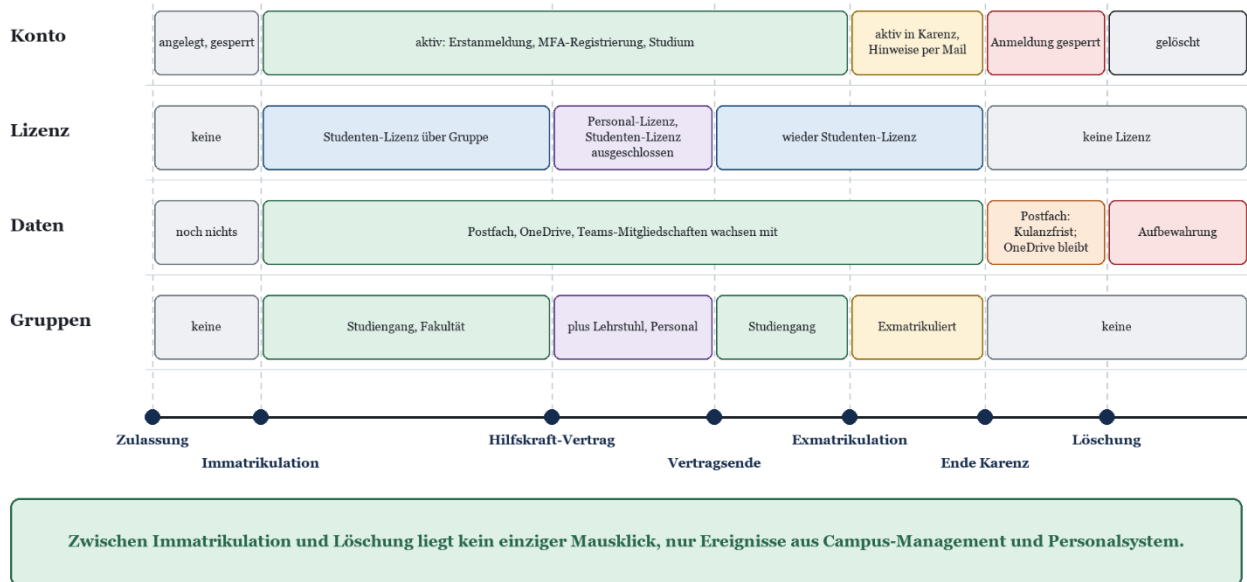
Übertragen auf die Hochschule ist das die typische Situation bei studentischen Hilfskräften: Die Doppelung entsteht nicht in Entra ID, sondern im Abgleich zwischen Campus-Management und Personalsystem. Dort muss sie auch beseitigt werden, und zwar bevor die Synchronisation sie nach Microsoft 365 trägt.

Die Lebenslinie eines Studentenkontos

Skizze 4 zeigt das Leben eines Studentenkontos als Zeitstrahl, und zwar an einem Beispiel mit Hilfskraftvertrag, weil der einfache Fall ohnehin niemanden überrascht. Vier Spuren laufen parallel: der Zustand des Kontos, die Lizenz, die Daten und die Gruppen. Jeder Wechsel in einer Spur lässt sich auf ein Ereignis in einem Quellsystem zurückführen.

Skizze 4: Lebenslinie eines Studentenkontos

Ein Student mit Hilfskraftvertrag im Studium. Vier Spuren, ein Zeitstrahl, und jeder Wechsel kommt aus einem Quellsystem.



Schematische Darstellung, nicht maßstabsgetreu. Karenz- und Aufbewahrungsfristen legt jede Hochschule selbst fest.

Immatrikulation und Erstanmeldung

Viele Hochschulen legen das Konto schon bei der Zulassung an, aber gesperrt, damit die Immatrikulation nicht auf die Technik warten muss. Mit der Immatrikulation wird das Konto freigeschaltet und landet in der Lizenzgruppe. Die Erstanmeldung ist der heikelste Moment im ganzen Lebenszyklus: Wer hier ein Initialkennwort per Brief verschickt, hat das Problem nur in die Post verlagert. Besser ist ein Selbstbedienungsweg über das Campus-Portal, in dem der Student sich bereits mit seinen Bewerbungsdaten ausgewiesen hat, oder ein befristeter Zugangspass, mit dem gleich die MFA registriert wird. Wie man die MFA für zehntausende Konten einführt, ohne dass das Helpdesk kollabiert, ist ein eigenes Thema; die Grundlage dafür wird hier gelegt.

Wer die Anmeldung an Microsoft 365 über den Shibboleth-IdP föderiert, hat bei der Erstanmeldung andere Sorgen: Das Konto muss in Entra ID existieren, bevor die erste föderierte Anmeldung ankommt, und die Kennungen beider Welten müssen zueinander passen. Die drei Architekturvarianten dafür beschreibt [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#).

Rückmeldung, Urlaubssemester und Fachwechsel

Während des Studiums passiert mehr, als man denkt. Die Rückmeldung zum nächsten Semester ist an vielen Hochschulen die Bedingung dafür, dass der Status bleibt. Bleibt sie aus, folgt nach Fristen, die das Landesrecht und die Einschreibeordnung festlegen, die Exmatrikulation, oft nach einer Mahnung. Das Konto sollte diesen Weg mitgehen, aber nicht vorausseilen: Eine Sperre wegen verspäteter Rückmeldung trifft genau die Studenten, die in diesem Moment ihr Postfach brauchen, um die Mahnung zu lesen.

Ein Urlaubssemester ändert am Konto in der Regel nichts. Ein Fachwechsel ändert die Gruppen, nicht das Konto. Ein Hochschulwechsel innerhalb desselben Bundeslandes ist dagegen ein Austritt und ein Eintritt in zwei verschiedenen Tenants, auch wenn der Student das anders empfindet.

Ereignisse, Quellen und Wirkungen im Überblick

Die folgende Tabelle ist der Kern jeder Lebenszyklus-Konzeption. Sie gehört in die Dokumentation, in die Abstimmung mit der Studentensekretariat, mit dem Personaldezernat und dem Datenschutzbeauftragten. Die Fristen sind Beispiele für Entscheidungen, die jede Hochschule selbst trifft; feste Werte von Microsoft sind ausdrücklich gekennzeichnet.

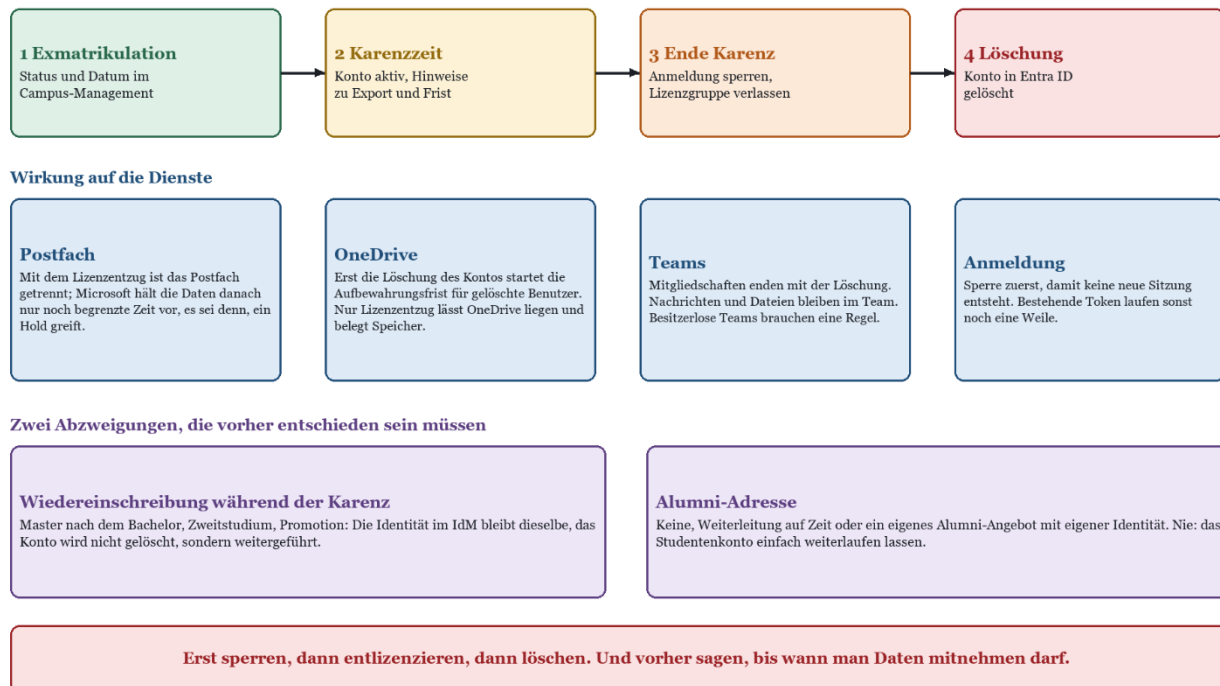
Ereignis	Quelle	Wirkung auf Konto	Wirkung auf Lizenz	Frist
Zulassung	Campus-Management	Konto angelegt, Anmeldung gesperrt	keine	mit dem Zulassungsbescheid
Immatrikulation	Campus-Management	Anmeldung freigegeben, Erstanmeldung mit MFA-Registrierung	Aufnahme in Studenten-Lizenzgruppe	sofort, spätestens zum Vorlesungsbeginn
Rückmeldung	Campus-Management	keine Änderung	keine Änderung	laufend
Fehlende Rückmeldung	Campus-Management	Hinweis, keine Sperre bis zur Exmatrikulation	keine Änderung	nach Einschreibeordnung
Urlaubssemester	Campus-Management	keine Änderung	keine Änderung	Hochschulregelung
Fachwechsel	Campus-Management	Gruppen wechseln, Konto bleibt	keine Änderung	zum Semester
Hilfskraftvertrag beginnt	Personalsystem	Personalrolle ergänzt, Lehrstuhlgruppen hinzu	Personal-Lizenz; Studenten-Lizenz per Regel ausgeschlossen	Vertragsbeginn
Hilfskraftvertrag endet	Personalsystem	Personalrolle entfernt, Lehrstuhlgruppen entfernt	erst Studenten-Lizenz, dann Personal-Lizenz entfernen	Vertragsende, Übergabe vorher
Exmatrikulation	Campus-Management	Konto bleibt aktiv, Hinweise zur Karenzzeit	keine Änderung während der Karenz	Karenzzeit nach Hochschulregelung
Ende der Karenzzeit	IdM (Frist)	Anmeldung gesperrt, Teams-Mitgliedschaften entfernt	Austritt aus Lizenzgruppe; Postfach danach nur noch 30 Tage wiederherstellbar (Microsoft)	Hochschulregelung
Löschung	IdM (Frist)	Konto in Entra ID gelöscht, 30 Tage im Papierkorb (Microsoft)	keine Lizenz mehr	Hochschulregelung, OneDrive-Aufbewahrung danach nach Tenant-Einstellung
Wiedereinschreibung	Campus-Management	dieselbe Identität, Konto wird weitergeführt	wieder Studenten-Lizenzgruppe	solange das Konto noch nicht gelöscht ist

Austritt: Exmatrikulation, Vertragsende und das Alumni-Konto

Eintritte merkt man, weil sich jemand beschwert, wenn sie nicht funktionieren. Austritte merkt niemand, und deshalb funktionieren sie an vielen Hochschulen nicht. Das Ergebnis sieht man in jeder Tenant-Prüfung: zehntausende Konten ehemaliger Studenten, manche noch mit Lizenz, viele mit Postfach, einige mit funktionierendem Kennwort und ohne MFA. Für Angreifer sind das die besten Konten überhaupt, denn niemand vermisst sie und niemand liest die Warnmails.

Skizze 5: Was nach der Exmatrikulation passiert

Ein Ereignis im Campus-Management, mehrere Fristen in Microsoft 365. Die Reihenfolge entscheidet, ob Daten geordnet verschwinden oder zufällig.



Schematische Darstellung. Fristen nach Microsoft-Standard und Hochschulregelung, Stand der Recherche 10/2026.

Die Karenzzeit

Nach der Exmatrikulation sofort alles abzuschalten, wäre technisch sauber und menschlich grausam. Es gibt gute Gründe für eine Karenzzeit: Zeugnisse und Bescheinigungen kommen noch per Mail, Abschlussarbeiten liegen in OneDrive, Bewerbungen laufen über die Hochschuladresse, und manchmal stellt sich heraus, dass die Exmatrikulation ein Irrtum war. Wie lang die Karenzzeit ist, entscheidet die Hochschule; Hochschulgesetze, Einschreibeordnungen und Löschkonzepte setzen dafür in jedem Bundesland einen etwas anderen Rahmen. Üblich sind Zeiträume von einigen Wochen bis zu wenigen Monaten.

Wichtig ist, dass die Karenzzeit kommuniziert wird, und zwar mehrfach: bei der Exmatrikulation, zur Hälfte der Frist und kurz vor ihrem Ende. Jede dieser Nachrichten sollte sagen, bis wann man Daten exportieren kann, wie das geht und was danach passiert. Ohne diese Hinweise wird die Karenzzeit zur Falle: Der ehemalige Student merkt erst beim nächsten Login, dass seine Masterarbeit nicht mehr da ist.

Was mit dem Postfach passiert

Exchange Online reagiert auf den Lizenzentzug sofort. Ein Benutzerpostfach ohne Hold wird getrennt, sobald die Exchange-Lizenz entfällt. Die Daten hält Microsoft danach 30 Tage vor; wird die Lizenz in dieser Zeit wieder zugewiesen, ist das Postfach vollständig zurück. Danach ist es endgültig weg. Wer Postfächer ehemaliger Studenten länger aufbewahren muss, braucht dafür eine

bewusste Aufbewahrungsrichtlinie oder einen Hold, und muss begründen können, warum. Bei Studentenkonten ist die Antwort meist: Es gibt keinen Grund.

Für große Tenants bietet Microsoft zusätzlich eine Schutzfunktion gegen versehentlichen Lizenzentzug. Sie verzögert die Wirkung eines Lizenzentzugs auf Exchange Online um weitere 30 Tage und steht laut Microsoft nur Tenants mit mehr als 5.000 nicht testweisen Lizenzen offen. Für einen Hochschul-Tenant klingt das verlockend, verändert aber den Ablauf: Ist sie aktiv, muss ein gewollter Lizenzentzug ausdrücklich beschleunigt werden, sonst läuft das Postfach exmatrikulierter Studenten einen Monat länger als geplant.

Was mit OneDrive passiert

Bei OneDrive ist die Logik eine andere, und genau das überrascht viele. Der Lizenzentzug allein startet keinen Löschmod. Erst wenn das Konto in Entra ID gelöscht wird, beginnt die Aufbewahrungsfrist für OneDrive. Sie beträgt standardmäßig 30 Tage und lässt sich im SharePoint Admin Center verlängern. In dieser Zeit erhält der im Konto eingetragene Vorgesetzte Zugriff, alternativ ein festgelegter sekundärer Besitzer, sofern die Zugriffsdelegation eingeschaltet ist. Danach wandert das OneDrive in den Papierkorb der Websitesammlung und ist nach weiteren 93 Tagen endgültig gelöscht, sofern keine Aufbewahrungsrichtlinie oder kein Hold das verhindert.

Bei Studenten ist das Feld für den Vorgesetzten meist leer, und das ist auch richtig so. Die Folge ist allerdings, dass niemand automatisch Zugriff bekommt und niemand gewarnt wird, sofern kein sekundärer Besitzer eingetragen ist. Für Studentenkonten ist das in der Regel gewollt. Für Konten von Hilfskräften und Personal ist es das nicht; dort gehört ein Vorgesetzter ins Konto, und die Übergabe der dienstlichen Daten gehört vor das Vertragsende, nicht danach.

FAKTEN · OneDrive ohne Lizenz im Education-Tenant

Microsoft hat für kommerzielle Tenants eine Regel eingeführt, nach der OneDrive-Konten ohne Lizenz nach 60 Tagen schreibgeschützt und nach 93 Tagen kostenpflichtig archiviert werden. Diese Regel gilt laut Microsoft ausdrücklich nicht für Education-Kunden. Als Education-Tenant zählt ein Tenant, in dem mehr als die Hälfte der Lizenzen Education-Lizenzen sind.

Das ist kein Freibrief. Auch im Education-Tenant belegen OneDrive-Konten ohne Lizenz Speicher aus dem gemeinsamen Pool und bleiben ein Sicherheits- und Datenschutzthema. Das SharePoint Admin Center zeigt sie in einem eigenen Bericht. Ein Konto, das nur entlizenziert, aber nie gelöscht wird, ist kein Abschluss, sondern ein Dauerzustand.

Was mit den Teams-Mitgliedschaften passiert

Kursteams, Projektteams und Fachschaftsteams überleben ihre Mitglieder. Wird das Konto gelöscht, verschwindet die Mitgliedschaft; Nachrichten und Dateien bleiben im Team. In Chats und Kanälen erscheint der ehemalige Student danach als unbekannter oder entfernter Benutzer. Das ist richtig so, denn die Inhalte gehören zum Team und nicht zur Person.

Kritisch sind zwei Fälle. Erstens Teams, in denen der ausscheidende Student der einzige Besitzer war, etwa bei einer studentischen Initiative oder einem Projekt, das ein Doktorand angelegt hat. Microsoft 365 kennt dafür eine Richtlinie für besitzerlose Gruppen, die Mitglieder auffordert, die Besitzerrolle zu übernehmen; einschalten müssen Sie sie selbst. Zweitens Freigaben aus dem OneDrive des Ausscheidenden in Teams hinein: Mit dem OneDrive verschwinden auch die Dateien, auf die im Kanal verlinkt wurde. Was im Team weiterleben soll, gehört in die Dateiablage des Teams, nicht ins persönliche OneDrive.

Ob Mitgliedschaften schon am Ende der Karenzzeit oder erst mit der Löschung enden, ist eine Entscheidung. Für Kursteams spricht einiges dafür, sie früh zu bereinigen, damit Dozenten in ihren Teams nicht dauerhaft die Namen von Studenten sehen, die längst woanders arbeiten.

Vertragsende beim Personal

Beim Personal ist das Vertragsende planbar, weil es im Personalsystem steht. Befristungen im wissenschaftlichen Bereich enden aber oft nicht so, wie sie geplant waren: Ein Drittmittelvertrag wird kurzfristig verlängert, eine Anschlussbeschäftigung kommt einen Monat später, eine Elternzeit verschiebt alles. Das IdM sollte deshalb nicht am Vertragsende sofort löschen, sondern eine kurze Übergangsfrist kennen, in der das Konto gesperrt, aber vollständig erhalten bleibt. Die Übergabe dienstlicher Daten aus Postfach und OneDrive gehört vor diesen Termin, und zwar in die Verantwortung von Lehrstuhl oder Institut.

Für Personalkonten gilt zusätzlich, dass Protokolle über Anmeldungen und Kontoänderungen Daten über Mitarbeiterinnen und Mitarbeiter sind. Was davon wie lange gespeichert und wofür verwendet wird, gehört in die Dienstvereinbarung; Details dazu finden Sie in [Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle](#). Für Emeriti, Gastwissenschaftler und Lehrbeauftragte gelten eigene Regeln, die über die dritte Erfassung für Sonderrollen laufen.

Alumni-Adresse: ja oder nein?

Irgendwann fragt das Alumni-Büro, ob die Hochschuladresse nicht lebenslang bleiben könnte. Das Anliegen ist verständlich, und der Wunsch nach Verbundenheit mit der Hochschule ist ehrenwert. Technisch und rechtlich ist das Studentenkonto dafür aber das falsche Werkzeug. Es trägt eine Studentenlizenz, an der Nutzungsbedingungen hängen, es hat Zugriff auf interne Dienste, und es lebt in einem Tenant, dessen Sicherheitsniveau sich an aktiven Mitgliedern orientiert. Ein Konto, das zwanzig Jahre lang niemand mehr fachlich betreut, ist ein Sicherheitsrisiko mit Hochschulwappen.

Variante	Was der Alumnus bekommt	Vorteile	Nachteile
Keine Alumni-Adresse	nichts, nach der Karenzzeit ist Schluss	einfach, sauber, kein Restrisiko	Alumni-Büro unglücklich; Kontakt läuft über private Adresse
Weiterleitung auf Zeit	Mails an die alte Adresse gehen für eine begrenzte Zeit an eine private Adresse	Übergang ohne verlorene Post	Weiterleitung ohne Konto braucht ein Mail-Objekt im Tenant und eine klare Endfrist; Datenschutz der weitergeleiteten Inhalte klären
Eigenes Alumni-Angebot	Alumni-Portal oder Verteiler mit eigener Identität, eventuell eigene Domäne	trennt Alumni sauber vom Hochschulbetrieb	eigener Betrieb, eigene Lizenzfrage; Microsoft-Lizenzbedingungen für Alumni vorher prüfen
Studentenkonto weiterlaufen lassen	alles wie bisher	keine	Lizenzverstoß wahrscheinlich, Sicherheitsrisiko sicher, Löschkonzept ausgehebelt

Unsere Empfehlung ist schlicht: Das Studentenkonto endet nach der Karenzzeit. Wer Alumni etwas bieten will, baut ein eigenes Angebot mit eigener Identität, eigener Domäne und eigener Verantwortung, gern in Zusammenarbeit mit dem Alumni-Büro. Ob dafür überhaupt eine Microsoft-Lizenz in Frage kommt, ist eine Frage an die Education-Lizenzbedingungen und an Ihren Vertrag, nicht an die Technik.

HINWEIS · Kein Ersatz für die rechtliche Prüfung

Wie lange Daten ehemaliger Studenten und ehemaliger Mitarbeiterinnen und Mitarbeiter aufbewahrt werden dürfen oder müssen, regeln Hochschulgesetze, Landesdatenschutzgesetze, Einschreibe- und Prüfungsordnungen sowie das Personalaktenrecht. Diese Regeln unterscheiden sich zwischen den Bundesländern und zum Teil zwischen Hochschulen eines Landes. Für außeruniversitäre Forschungseinrichtungen kommen Satzungen und Tarifwerke hinzu.

Dieser Beitrag beschreibt die technischen Abläufe in Microsoft 365. Er ersetzt weder das Löschkonzept der Hochschule noch die Abstimmung mit dem Datenschutzbeauftragten und, für Personalkonten, mit dem Personalrat. Hintergründe zur Datenschutzseite finden Sie in:

[Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und Campus-Realität](#)

WICHTIG · Reihenfolge schlägt Werkzeug

Bei Austritten entscheidet die Reihenfolge darüber, ob Daten geordnet oder zufällig verschwinden. Bewährt hat sich: Hinweise während der Karenz, dann Anmeldung sperren und Sitzungen widerrufen, dann aus Lizenz- und Teamgruppen entfernen, dann nach einer weiteren Frist das Konto löschen. Wer zuerst löscht, verliert die Möglichkeit, einen Fehler rückgängig zu machen. Wer nie löscht, behält einen Bestand, den niemand mehr erklären kann.

Für Forschungseinrichtungen ohne Studenten sieht die Kette einfacher aus, weil das Campus-Management fehlt. Gäste, Stipendiaten und Mitarbeiter in Verbundprojekten machen den Lebenszyklus dort aber nicht leichter; die Besonderheiten der Institute beschreibt [Microsoft 365 in außeruniversitären Forschungseinrichtungen: Institute zwischen Zentrale und Eigenständigkeit](#). Wer den Lebenszyklus im Rahmen einer Microsoft-365-Einführung von Grund auf neu denkt, findet in [Microsoft-365-Einführung an der Hochschule: Konzeptionsphase in 4,5 Tagen und die Vorlage fürs Präsidium](#) den passenden Rahmen. Und wer dafür Unterstützung von außen sucht, ist mit der [Microsoft-365-Beratung für Hochschulen und Forschung](#) richtig.

FAQ: Identity Lifecycle an der Hochschule

Brauchen wir für Microsoft 365 ein neues Identity-Management-System?

In aller Regel nicht. Das vorhandene IdM bleibt das Personenregister und bekommt ein weiteres Ziel: Entra ID, entweder über das Active Directory und eine Synchronisation oder direkt über eine Schnittstelle. Neu zu bauen sind meist die Regeln für Lizenzgruppen, Fristen und Doppelrollen, nicht das System selbst.

Entra Connect oder Cloud Sync?

Beides funktioniert an Hochschulen. Entra Connect ist ausgereift und bietet viele Regelmöglichkeiten, verlangt aber einen eigenen Server und Erfahrung bei Regeländerungen. Cloud Sync ist leichter zu betreiben. Prüfen Sie den Funktionsumfang vor der Entscheidung gegen Ihre Anforderungen, etwa für Exchange-Hybrid oder besondere Attributflüsse.

Warum nicht einfach alle Konten von Hand im Admin Center pflegen?

Weil es zum Semesterstart nicht funktioniert und am Semesterende niemand daran denkt. Handarbeit erzeugt fehlende Lizenzen, doppelte Lizenzen und Konten, deren Herkunft niemand mehr kennt.

Können Studenten und Personal unterschiedliche Domänen haben?

Ja, und viele Hochschulen machen das. Bei Doppelrollen braucht es dann eine Rangfolge für die primäre Adresse. Ob auch der Anmeldename an der Rolle hängt, sollte früh entschieden werden, weil jede spätere Änderung am Anmeldennamen Aufwand bei Benutzern und Helpdesk erzeugt.

Was passiert, wenn ein exmatrikulierter Student sich wieder einschreibt?

Ist das Konto noch nicht gelöscht, führt das IdM es mit derselben Identität weiter. Ist es gelöscht, hält Entra ID gelöschte Benutzer 30 Tage im Papierkorb. Danach entsteht ein neues Konto ohne die alten Daten. Deshalb sollte die Identität im IdM länger leben als das Konto in Entra ID.

Wie lange bleibt das Postfach nach dem Lizenzentzug erhalten?

Ohne Hold trennt Exchange Online das Postfach mit dem Lizenzentzug und hält die Daten noch 30 Tage zur Wiederherstellung vor. Danach ist es endgültig gelöscht. Ist die Schutzfunktion gegen versehentlichen Lizenzentzug aktiv, verlängert sich der Zeitraum.

Wird OneDrive automatisch gelöscht, wenn die Lizenz entfällt?

Nein. Der Löschprozess beginnt erst, wenn das Konto in Entra ID gelöscht wird. Ein nur entlizenziertes OneDrive bleibt bestehen und belegt im Education-Tenant Speicher aus dem gemeinsamen Pool.

Sollten Alumni ihre Hochschuladresse behalten?

Nicht über das Studentenkonto. Wer Alumni eine Adresse anbieten will, sollte das als eigenes Angebot mit eigener Identität und klärender Lizenzprüfung aufbauen. Eine befristete Weiterleitung ist ein vernünftiger Kompromiss.

Wer entscheidet über die Länge der Karenzzeit?

Die Hochschule, im Rahmen von Landesrecht, Einschreibeordnung und Löschkonzept. Das Rechenzentrum setzt die Frist technisch um, sollte sie aber nicht allein festlegen. Beteiligt sind typischerweise Studentensekretariat, Datenschutzbeauftragter und, wo es um Personal geht, der Personalrat.

Fazit: Ein Konto ist ein Versprechen mit Ablaufdatum

Identity Management an der Hochschule mit Entra ID ist kein Produktthema, sondern ein Prozessthema mit Durchsatzanforderung. Die Technik ist vorhanden: Quellsysteme, ein IdM, das Personen zusammenführt, ein Active Directory oder eine Schnittstelle, eine Synchronisation und gruppenbasierte Lizenzen. Was fehlt, sind an vielen Hochschulen die Regeln dazwischen, also wer führend ist, wie Doppelrollen aufgelöst werden und in welcher Reihenfolge ein Konto stirbt.

Wer diese Regeln einmal sauber festlegt, erlebt den nächsten Semesterstart deutlich entspannter. Wer sie nicht festlegt, erlebt ihn wie jedes Jahr, nur mit einem weiteren Dienst, der am ersten Tag nicht funktioniert. Und das Alumni-Konto? Das ist meistens das Konto, das man am besten gar nicht erst anlegt. Die Erinnerung an die Hochschule hält auch ohne Postfach.

WEITERLESEN · Weiterlesen

Die Serie zu Microsoft 365 in Hochschule und Forschung. Für diesen Beitrag besonders passend:

- › [Microsoft 365 in Hochschule und Forschung](#)
- › [Entra ID und Shibboleth: Microsoft 365 an die DFN-AAI-Welt anbinden](#)
- › [Education-Lizenzen verstehen: A1, A3, A5 und der Student Use Benefit](#)
- › [Microsoft 365 an Hochschulen: Wo der Campus anders tickt als Verwaltung und Wirtschaft](#)
- › [Dezentrale IT an der Hochschule: Lehrstuhl-Admins, Fakultäts-IT und ein Tenant für alle](#)
- › [Datenschutz und Microsoft 365 an Hochschulen: Zwischen DSK-Bewertung, Landesaufsicht und](#)

Campus-Realität

- › Personalrat und Microsoft 365 an der Hochschule: Dienstvereinbarung, wissenschaftliches Personal und die Verhaltenskontrolle
- › Microsoft-365-Beratung für Hochschulen und Forschung
- › Microsoft-365-Schulung für Hochschulen und Forschungseinrichtungen