FH | JOANNEUM
University of Applied Sciences

IT - Ordnung

Rev.	Gültig ab	Erstellt / Rolle	Anmerkung / Änderung
01	06.07.2015	Gerhard Maxl / ZIT	Erste Ausgabe
02	08.03.2019	Gerhard Maxl / ZIT	Punkt 8.4 wurde ergänzt, Punkt 4.6 wurde ersatzlos gestrichen.
03	02.06.2020	Gerhard Maxl / ZIT	Alle Punkte, die die Nutzung von persönlichen Z-Laufwerken betreffen, wurden um „persönliche Cloud-Speicherplätze“ ergänzt. Alle Punkte, die die Nutzung von Netzlaufwerken betreffen, wurden um „Cloud-Speicherplätze“ ergänzt.
04	14.09.2022	Gerhard Maxl / ZIT	„Multifaktor-authentifizierung“ wurde ergänzt.
05	13.12.2023	Gerhard Maxl / ZIT	Komplette Überarbeitung und Zusammenführung mit dem Dokument „Aktivierung, Deaktivierung und Löschung von Benutzerkonten“.
06	03.12.2024	Gerhard Maxl / ZIT	Änderung der Gültigkeit bei Alumni - Accounts
07	30.09.2025	Gerhard Maxl / ZIT	Ergänzungen zu den Themen Benutzerkonten, Passwortsicherheit und mobiles Arbeiten

Corinna Engelhardt-Nowitzki / GEF

Corinna Engelhardt-Nowitzki, 14.10.2025 21:29
Rektorin (FH), Wissenschaftliche Geschäftsführerin
FH JOANNEUM Gesellschaft mbH

Martin Payer / GEF

Martin Payer, 15.10.2025 13:02
Kaufmännischer Geschäftsführer
FH JOANNEUM Gesellschaft mbH

Stand: 30.09.2025

INHALT

1. ZIEL / ZWECK

Die vorliegende IT-Ordnung wurde im Wissen um die Bedeutung des Funktionierens aller IT-Einrichtungen der FH JOANNEUM konzipiert und zielt mit allen Geboten und Verboten auf die Erreichung dieses Zieles ab, um für alle an der FH JOANNEUM Tätigen möglichst optimale Arbeitsbedingungen zu schaffen.

Die FH JOANNEUM stellt den Benutzer:innen für die Durchführung von IT-Aktivitäten, welche die Aufgabenbereiche von Lehre, Forschung und Verwaltung betreffen, IT-Systeme (Hardware, Software, Cloud Services) und das IT-Netzwerk des Unternehmens zur Verfügung.

Alle Benutzer:innen sind zur Einhaltung der vorliegenden IT-Ordnung verpflichtet. Vorgesetzte und Studiengangsleiter:innen tragen nach Maßgabe ihrer Möglichkeiten für die Einhaltung durch die Benutzer:innen Sorge. Für den Fall, dass Bestimmungen der vorliegenden IT-Ordnung von einzelnen Benutzer:innen nicht berücksichtigt werden, kann die Nutzungsberechtigung der/des jeweilig betreffenden Benutzers:in ungeachtet weiterer dienstrechtlicher Konsequenzen eingeschränkt, auf bestimmte Zeit suspendiert oder gänzlich entzogen werden.

2. GÜLTIGKEIT UND GELTUNGSBEREICH

Die vorliegende IT-Ordnung in der jeweils gültigen Fassung gilt für alle Benutzer:innen. Benutzer:innen im Sinne dieser Regelungen sind alle Studierenden, internen und externen Lehrenden und sonstige Mitarbeiter:innen der FH JOANNEUM.

3. BENUTZERKONTEN

3.1 ZEITLICHE ABGRENZUNG

Die Benutzer:innen erhalten die Nutzungsberechtigung für die IT-Einrichtungen der FH JOANNEUM grundsätzlich vom Tag ihres Eintrittes bis zum Tag ihres Austrittes. Darüber hinaus gehend sind folgende Zeiträume bis zur Deaktivierung und Löschung der Zugänge zu den IT-Einrichtungen, sowie für die Aufbewahrungsdauer von Daten definiert:

Deaktivierungstabelle - Benutzerkonten

Funktion	Maßnahme	Deaktivierung nach (in Tagen)
Studierende	Änderung des Studienzustandes auf Absolvent:in (es gilt hier der Tag der erfolgreichen Abschlußprüfung)	365
Studierende	Änderung des Studienzustandes auf Studienabbrecher:in	7
Incomings	Änderung des Studienzustandes auf Incoming-Abgänger:in	90
Fixangestellte Mitarbeiter:innen	Austrittsdatum erreicht	1
Externe Lehrbeauftragte	Austrittsdatum erreicht	300

Löschungstabelle - Benutzerkonten

Funktion	Maßnahme	Löschung nach (in Tagen)
Studierende	Änderung des Studienzustandes auf Absolvent:in (es gilt hier der Tag der erfolgreichen Abschlußprüfung)	365
Studierende	Änderung des Studienzustandes auf Studienabbrecher:in	14
Incomings	Änderung des Studienzustandes auf Incoming-Abgänger:in	90
Fixangestellte Mitarbeiter:innen	Austrittsdatum erreicht	30
Externe Lehrbeauftragte	Austrittsdatum erreicht	300

Mit der Löschung des Benutzerkontos werden auch der Benutzername, das Passwort und zeitgleich die Daten auf den persönlichen Speicherplätzen, bzw. auf dem persönlichen Cloud-Speicherplatz, sowie die E-Mails der betreffenden Person gelöscht.

3.2 PASSWÖRTER

Passwörter sind in jedem Fall geheim zu halten. Temporäre oder Initial-Anmeldeinformationen sind beim ersten Login zu ändern.
Passwörter müssen den jeweils aktuellen Vorgaben (Passwort Policy) entsprechen.

Den Mitarbeiter:innen ist es daher ausnahmslos untersagt, das Passwort an andere Personen weiterzugeben oder in irgendeiner Form für andere Personen zugänglich zu notieren. Die Verwaltung und Speicherung der Passwörter ist ausschließlich in, von der ZIT empfohlenen Software-Tools (z.B. Passbolt), erlaubt. Es ist dahingehend Sorge zu tragen, dass das Passwort bei der Eingabe nicht „von den Fingern" abgelesen werden kann.

Jede(r) Mitarbeiter:in ist für ihr/sein Passwort und alle Eingaben in die IT-Systeme, die unter diesem Benutzerkonto getätigt werden, verantwortlich.
Sollte der Verdacht bestehen, dass das persönliche Passwort nicht mehr sicher ist, so ist das Passwort unverzüglich zu ändern und dieser Verdacht umgehend der Abteilung Zentrale IT-Services (ZIT) mitzuteilen.
Es ist untersagt, mit einem fremden Benutzerprofil zu arbeiten, es sei denn, es handelt sich um ein allgemeines Benutzerkonto, welches speziell für diesen Zweck freigegeben wurde. Im Falle eines Verstoßes gegen diese Vorschriften trägt die/der Verfügungsberechtigte über das jeweilige Benutzerkonto die Verantwortung für sämtliche daraus resultierende Schäden.

Passwörter, die leicht zu erraten sind, dürfen nicht verwendet werden. Zu vermeiden sind insbesondere: Zeichenwiederholungen, Zahlen und Daten aus dem Lebensbereich des Benutzers, Zeichenkombinationen, die nur unwesentlich von den vorherigen Passwörtern abweichen, einfache Ziffern- und Buchstabenkombinationen, Zeichen, die durch nebeneinanderliegende Tasten eingegeben werden und Zeichenkombinationen den Suchbegriffen in Wörterbüchern und Lexika entsprechen (Trivialpasswörter).

Passwörter müssen nach jedem Zurücksetzen geändert werden.

3.3 MULTIFAKTORAUTHENTIFIZIERUNG

Für definierte Benutzer:innengruppen (z.B.: Administrator:innen, Alumni, Studierende, Lehrende und Mitarbeiter:innen) ist zusätzlich zur Authentifizierung mittels Benutzername und Kennwort eine Multifaktorauthentifizierung vorgesehen. Dazu wird seitens der Abteilung Zentrale IT-Services (ZIT) die Verwendung einer Authentication-App am Smartphone oder ein Hardwaretoken (USB-Stick) empfohlen.

4. BENÜTZUNG DER IT-EINRICHTUNGEN

In den freien Übungszeiten kann grundsätzlich jede:r Studierende der FH JOANNEUM die für IT-Aktivitäten vorgesehenen Räume benutzen, sofern ein IT-Gerät frei ist. Ausdrücklich wird aber darauf hingewiesen, dass seitens der Abteilung Zentrale IT-Services (ZIT) keine Regelung dieser Benutzungszeiten erfolgt. Im Interesse aller Benutzer:innen wird daher gebeten, im Falle der Knappheit der vorhandenen Infrastruktur, die IT-Räume und die IT-Einrichtungen nur so lange zu benutzen, wie es für das freie Üben unbedingt notwendig ist.

4.1 FIRMENENDGERÄTE

Als Firmenendgerät wird Hardware bezeichnet, welche von der FH JOANNEUM den Mitarbeiter:innen zur Verfügung gestellt wurde. Geschäftshandys dürfen privat genutzt werden.

4.2 PRIVATE ENDGERÄTE

Als privates Endgerät wird Hardware bezeichnet, welche nicht von der FH JOANNEUM den Mitarbeiter:innen zur Verfügung gestellt wurde und somit nicht von der ZIT verwaltet wird.

Die Nutzung privater Endgeräte für betriebliche Zwecke (auch als BYOD – bring your own device bezeichnet) ist erlaubt. Hierfür wird den Benutzer:innen der externe Zugang ermöglicht (siehe Kapitel 5 „Mobiles Arbeiten“).

4.3 SCHUTZ VOR SCHADSOFTWARE

Auf jedem von der FH JOANNEUM verwalteten, bzw. beschafften IT-Endgerät (PC, Workstation, Notebook, Tablet, Smartphone) ist, je nach technischen Möglichkeiten ein End Point Security System installiert, welches von der Abteilung Zentrale IT-Services (ZIT) vorgegeben ist.

Auf allen nicht von der ZIT verwalteten Firmengeräten ist das von der ZIT in Produkt und Version vorgegebene End Point Security System zu installieren und zu aktivieren.

Auf privaten Endgeräten (PC, Notebook, Smartphone, etc.) mit denen die Benutzer:innen über den externen Netzwerkzugang im FH JOANNEUM-Netzwerk arbeiten, ist auf eigene Kosten ein aktueller Schadsoftwareschutz (Virenscanner) zu installieren und zu aktivieren. Die Benutzer:innen sind selbst dafür verantwortlich, dass ihr Endgerät gegen aktuelle bekannte Bedrohungen geschützt ist.

Alle Benutzer:innen sind in deren Bereichen dafür verantwortlich, dass eine „Vireninfektion“ bzw. die Installation von Schadsoftware verhindert wird. Besondere Vorsicht im Hinblick auf Schadsoftware ist beim Download von Dateien aus dem Internet bzw. beim Empfang von E-Mails mit Dateianhängen geboten. Wechselmedien (USB-Sticks, externe Festplatten, etc.) dürfen nur verwendet werden, wenn ausgeschlossen werden kann, dass Schadsoftware darauf ist. Ein offensichtlich von einer Schadsoftware befallenes Medium darf keinesfalls verwendet werden, ohne dass vorher die Beseitigung der Schadsoftware durch die Abteilung Zentrale IT-Services (ZIT) erfolgt ist.

Die FH JOANNEUM behält sich vor, bei Gefahr in Verzug eine sofortige Sperre des Netzwerkzugangs vorzunehmen. Weiters behält sich die FH JOANNEUM ausdrücklich das Recht vor, Aktivitäten der Benutzer:innen im FH JOANNEUM-Netzwerk im Rahmen der gesetzlich zulässigen Bestimmungen mitzuprotokollieren und gegebenenfalls auszuwerten.

4.4 SCHUTZ VOR UNBEFUGTER NUTZUNG

Alle Firmenendgeräte und privaten Endgeräte, die Zugriff auf das Firmennetzwerk haben (auch private Smartphones mit eingerichteter Synchronisation von Firmendaten, z.B. E-Mails), müssen im Standby gesperrt sein bzw. wenn diese nicht beaufsichtigt sind, müssen diese gesperrt werden. Zum Entsperren muss das Account-Passwort eingegeben werden. Alternativ kann auch ein Fingerprint oder ein anderes biometrisches Merkmal eingestellt werden.

Alle Benutzer:innen haben sich nach der Beendigung ihrer Arbeiten an der verwendeten IT-Einrichtung wieder abzumelden. Bei Verlassen des Arbeitsplatzes ist die Arbeitsstation zu sperren, bei längerer Abwesenheit hat jedenfalls eine Abmeldung zu erfolgen.

Innerhalb des Unternehmens hat die letzte Person, die den Raum verlässt, die Bürotür zuzusperren. Sowohl Smartphones als auch die Festplatten der Notebooks sind durch eine Verschlüsselung gegen eine unberechtigte Einsichtnahme zu schützen.

Es ist dafür Sorge zu tragen, dass keine unbefugte Person Einsicht auf vertrauliche Informationen erhält. Dies gilt besonders auf öffentlichen Plätzen und Verkehrsmitteln, aber auch beim Kunden. Bei Bedarf einer Sichtschutzfolie kann diese beim direkten Vorgesetzten beantragt werden.

5. EXTERNER ZUGANG – MOBILES ARBEITEN

Die FH JOANNEUM ermöglicht ihren Benutzer:innen, jeweils für die Dauer ihres Studiums bzw. für die Dauer ihres Dienstverhältnisses, den externen Zugang zum FH JOANNEUM-Netzwerk über das Internet.

Der externe Netzwerkzugang darf keinesfalls betriebsfremden Personen zugänglich gemacht werden.

Zur Verbindungsaufnahme sind folgende Authentifizierungsmaßnahmen erforderlich:

- VPN mit Multifaktorauthentifizierung für firmeninterne Anwendungen/Laufwerke
- EntraID mit Multifaktorauthentifizierung für Anwendungen in der Microsoft-Cloud

Die FH JOANNEUM ist von jedem Schaden freizuhalten, der durch die ins Netz gebrachten Daten oder durch die dem Netz entnommenen Daten entsteht oder entstehen könnte.

Projekt-Daten müssen auf zentrale Speichermedien (Projektlaufwerke, Projektteams gesichert werden, nur so kann die Verfügbarkeit garantiert und im Bedarfsfall Daten zurückgespielt werden. Für ein Back-up sonstiger Daten auf dem Notebook ist der Nutzer selbst verantwortlich.

Die Nutzung von mobilen Firmenendgeräten durch firmenfremde Personen (z.B.: Familienmitglieder) ist untersagt.

5.1 SCHUTZ VOR DIEBSTAHL

Alle mobilen Firmenendgeräte (Notebooks, Smartphones, o.Ä.) müssen sowohl innerhalb als auch außerhalb des Unternehmens sicher gegen Diebstahl verwahrt werden. Firmenendgeräte sollten z.B.: nicht sichtbar in einem Fahrzeug aufbewahrt werden, selbst wenn das Fahrzeug versperrt ist.

5.2 VERLUST EINES MOBILEN FIRMENGERÄTES

Der Verlust eines Notebooks, Handys oder Smartphones ist umgehend an den ZIT-Support zu melden. Sollten mobile Geräte oder mobile Datenträger innerhalb des Unternehmens aufgefunden werden, sind diese in der ZIT abzugeben.

Geht ein mobiles Gerät mit offenem Zugang zum Firmennetzwerk verloren, ist umgehend das Kennwort des Accounts zu ändern und eine Meldung an den ZIT-Support zu senden. In einem solchen Fall behält sich das Unternehmen das Recht vor, die Daten remote zu löschen, um zu verhindern, dass Daten auf dem Gerät an Dritte gelangen könnten.

5.3 PHYSISCHE SICHERHEIT

Es ist auf einen sorgfältigen Umgang bei Transport und Aufstellung von Firmengeräten zu achten (z.B. Schutztasche verwenden, Vermeidung direkter Sonneneinstrahlung, Schutz vor Nässe).
Hardware-Veränderungen an den Firmen-Notebooks dürfen nur nach Genehmigung der ZIT erfolgen.

6. WEBAUFTRITTE

Jeder Webauftritt der FH JOANNEUM oder in der Verantwortung der FH JOANNEUM muss folgende Voraussetzungen erfüllen:

Ein Impressum (siehe https://www.fh-joanneum.at/hochschule/organisation/impressum/), ausgenommen Studierendenprojekte im Rahmen einer LV (diese müssen als Impressum den Studierenden anführen).

Datenschutzerklärung (siehe https://www.fh-joanneum.at/hochschule/organisation/datenschutz/), ausgenommen Studierendenprojekte im Rahmen einer LV (diese muss vom Studierenden erstellt werden).

Bei Verwendung von technisch nicht notwendigen Cookies ist ein sogenannter Cookie-Banner verpflichtend (in Verbindung mit einer dementsprechenden Policy).

7. VERPFLICHTUNGEN DER BENUTZER:INNEN

Die Benutzerverwaltung erfolgt ausschließlich von der Abteilung Zentrale IT-Services der FH JOANNEUM (ZIT).

Die Beschaffung von IT-Einrichtungen wird ausschließlich von oder in Abstimmung mit der ZIT durchgeführt.

Der Support der IT-Einrichtungen der FH JOANNEUM wird ausschließlich von Mitarbeiter:innen der ZIT oder von nachweislich durch FH JOANNEUM befugte Personen durchgeführt.

Jegliche Änderung von Hard- und Software-Konfigurationen sämtlicher IT-Einrichtungen obliegt ausschließlich Mitarbeiter:innen der ZIT bzw. Personen, die durch die ZIT autorisiert wurden.

Die Verlagerung von IT-Einrichtungen an einen anderen Standort darf ausnahmslos nur mit Zustimmung der ZIT erfolgen, soweit die Geräte nicht für den mobilen Betrieb bestimmt sind.

Alle Benutzer:innen der IT-Einrichtungen der FH JOANNEUM akzeptieren, dass die ZIT bei Gefahr in Verzug, wie z.B. beim Auftreten von Viren oder bei begründetem Verdacht von Verstößen gegen die vorliegenden IT-Ordnung, berechtigt ist, sämtliche Daten der Benutzer:innen zu analysieren und gegebenenfalls die Berechtigungsstruktur zu verändern. Die Betroffenen werden jedenfalls davon verständigt.

Bei Schäden an oder Abhandenkommen von IT-Einrichtungen ist die ZIT unverzüglich zu verständigen. Alle Benutzer:innen haften für die von ihnen schuldhaft verursachten Schäden.

Daten und/oder Informationen die Ihnen auf Grund einer technischen Störung und/oder einer Fehlbedienung zugänglich gemacht werden oder wurden, dürfen nicht eingesehen, kopiert oder verteilt werden, sofern Sie nicht der/die beabsichtigte Empfänger:in sind. Darüber hinaus werden Sie ersucht, sich mit der/dem Absender:in, bzw. mit der ZIT in Verbindung zu setzen.

8. PRIVATE NUTZUNG

IT-Hardware, Software, Internet, E-Mail, sowie Sprach-, Video- und Chat-Dienste (zB. MS-Teams) sind für berufliche bzw. Ausbildungszwecke einzusetzen. Eine Nutzung zu privaten Zwecken ist unverbindlich bis auf weiteres gestattet, sofern folgende Punkte eingehalten werden:

Die beanspruchten Ressourcen (Arbeitszeit, Netzwerkkapazität, Bandbreite, Speicherplatz usw.) müssen vernachlässigbar sein und die private Nutzung darf die rechtmäßigen Interessen der FH JOANNEUM sowie im Fall von Mitarbeiter:innen die Erfüllung der ihnen zugewiesener Aufgaben nicht beeinträchtigen.

Mitarbeiter:innen haben für eine klare und saubere Trennung von privaten und beruflichen Inhalten zu sorgen. So sind insbesondere allfällige private Dateien in einem separaten und deutlich als „Privat" bezeichneten Ordner auf dem persönlichen Speicherplatz abzuspeichern. Entsprechende Maßnahmen sind auch bei der E-Mailnutzung zu setzen.

Jegliche Verwendung der IT-Einrichtungen der FH JOANNEUM für kommerzielle Zwecke, die nicht in Zusammenhang mit der Tätigkeit an der FH JOANNEUM stehen, ist generell und ohne Ausnahme unzulässig.

9. UNZULÄSSIGE VERWENDUNG

Alle Maßnahmen, um Sicherheitslücken und Angriffsmöglichkeiten in den IT-Systemen der FH JOANNEUM zu suchen und/oder auszunutzen, sind ausdrücklich verboten. Das Ausspionieren des Netzwerkverkehrs der FHJ ist verboten. Sicherheitsaudits dürfen ausschließlich von speziell dafür autorisierten Personen in Abstimmung mit der ZIT durchgeführt werden.

Es ist untersagt, die IT-Einrichtungen der FH JOANNEUM gegen deren Interessen zu nutzen.

Bei Verdacht auf eine unzulässige Verwendung der IT-Einrichtungen der FH JOANNEUM kann eine Einsichtnahme in Daten und Protokolle der Benutzerin / des Benutzers gemäß der Verfahrensanweisung „Einsichtnahme in Daten und Protokolle" beantragt werden.

Das Bedrucken von Kunststofffolien auf den Druckern, Kopierern und Plottern der FH JOANNEUM ist nicht gestattet. Kosten für Reparaturen oder Ersatzgeräte, welche durch ein Zuwiderhandeln entstehen, sind von den verursachenden Benutzer:innen zu tragen.

Es ist untersagt Software zu installieren oder zu kopieren, ohne nachweislich durch Mitarbeiter:innen der ZIT oder von diesen autorisierten Personen oder von Lehrenden berechtigt zu sein.

Es ist untersagt, nicht von FH JOANNEUM lizenzierte Software zu installieren oder auszuführen.

Die Verwendung von Streaming Diensten (z.B. Netflix, Youtube, usw.) ist nur zum Zwecke der Lehre und Forschung bzw. im betrieblichen Kontext zulässig.

Bei Verwendung von KI-Software (Künstliche Intelligenz) ist auf die Einhaltung von ethischen Grundwerten (zB.: Achtung der Menschenwürde, Freiheit des Einzelnen, Achtung von Demokratie, Gerechtigkeit und Rechtsstaatlichkeit, Gleichheit, Nichtdiskriminierung und Solidarität, Bürgerrechte) zu achten.