**Checkliste: IT-Offboarding**

## Private und geschäftliche Daten

Informieren Sie ausscheidende Mitarbeitende, dass sie ihre privaten Daten von Laptop, Datenspeicher auf dem Server und aus dem E-Mail-Account löschen sollen. Machen Sie auch klar, dass ohne Zustimmung keine geschäftlichen Daten, Dokumente, Ordner oder E-Mails gelöscht werden dürfen.

Wichtig: Daten oder E-Mails, die sich in einem Ordner «Privat» befinden, dürfen Sie als Arbeitgeber auch nach dem Austritt nicht einsehen, alle anderen Daten hingegen schon.

## Abwesenheitsnotiz und Weiterleitung für E-Mail und Telefon

Richten Sie für jede scheidende Mitarbeiterin eine Abwesenheitsnotiz ein.

*Sehr geehrte Damen und Herren*

*Vielen Dank für Ihre E-Mail. Frau XY ist nicht mehr für unser Unternehmen tätig. Bitte wenden Sie sich an info@firma.com.*

Statt eine Abwesenheitsnotiz aufzusetzen, können Sie auch veranlassen, dass alle E-Mails an einen anderen Mitarbeiter weitergeleitet werden. Auch Anrufe auf die Handy- und die Festnetznummer sollten für eine gewisse Zeit weitergeleitet werden.

## Kennwort ändern

Am letzten aktiven Arbeitstag sollte das Passwort für das Benutzerkonto geändert werden.

## Zugriffe auf Firmensoftware sperren

Sperren Sie vor oder nach dem Austritt der Mitarbeiterin ihre Zugriffe auf alle Softwareprodukte wie CRM-System, ERP-, Buchhaltungssystem etc. Sperren Sie zusätzlich allfällige Authentifizierungstoken ([2FA/MFA](https://www.gryps.ch/ratgeber/it-sicherheit-unternehmen/passwoerter/#176685)). Haben Sie physische Token ausgegeben – beispielsweise USB-Sticks, ohne die ein Zugang nicht möglich ist –, müssen diese bei Ende des Arbeitsverhältnisses zurückgegeben werden.

## Berechtigungen löschen

Der Zugriff des Benutzers auf Server, E-Mails, Cloud-Accounts (Dropbox, Storebox, Google Drive etc., aber auch Office365) und die VPN-Verbindung sollte am Tag des Austritts entfernt werden. Arbeiten Sie mit der Liste, die Sie [beim Onboarding erstellt](https://www.gryps.ch/ratgeber/risiko-mitarbeitende/datendiebstahl/#176802) haben. Je nach Situation empfiehlt sich auch, den Zugriff auf einzelne Ordner, Dokumente oder Programme bereits vor dem letzten Arbeitstag zu deaktivieren. So verhindern Sie böswilliges Löschen von Firmendaten.

## E-Mail-Konto deaktivieren und archivieren

Definieren Sie, wie lange die E-Mail-Adresse einer ausgetretenen Mitarbeiterin für die Aussenwelt aktiv bleiben soll. Üblich und sinnvoll sind ein bis drei Monate. Danach können die E-Mail-Adresse und die Benutzerin deaktiviert werden.

Legen Sie anschliessend den E-Mail-Account in einem separaten Ordner ab. Nach beispielsweise sechs Monaten archivieren Sie ihn auf einem Archivierungs-Back-up, und nach weiteren sechs Monaten kann er ganz gelöscht werden.

## Handyvertrag kündigen

Oft haben Ihre Mitarbeitenden einen eigenen Vertrag für das Geschäftshandy. Auch diese Kündigung sollten Sie nicht vergessen.

## Geräte zurücknehmen

Beim Eintritt des Mitarbeiters haben Sie alle abgegebenen Geräte wie Computer, Laptop, Harddisks, USB-Sticks und Handy [dokumentiert](https://www.gryps.ch/ratgeber/risiko-mitarbeitende/datendiebstahl/#176802). Beim Austritt dient Ihnen die Liste als Basis für die Rückgabe.

## Unternehmensdaten von privaten Geräten löschen

Falls eine Mitarbeiterin auch private Geräte für Firmenzwecke benutzt hat, stellen Sie sicher, dass alle Unternehmensdaten von diesen gelöscht werden.

## Erklärung zur Datenhoheit

Lassen Sie austretende Angestellte eine Erklärung unterzeichnen, in der sie zustimmen, dass alle Unternehmensdaten nach der Kündigung weiterhin Eigentum des Unternehmens sind und weder weitergegeben noch weiterverwendet werden dürfen.