XCUBITOR

CHECKLISTE 3 VON 3

Offboarding-Checkliste: Zugänge sauber entziehen

Wenn jemand das Unternehmen verlässt, bleiben im Schnitt mehr Zugänge offen, als irgendwer weiß. Diese Liste schließt sie – am letzten Tag, in der richtigen Reihenfolge, mit Nachweis.

Checkliste zum Ausdrucken und Ausfüllen · Stand: November 2026 · xcubitor.at

1 Vor dem letzten Tag

Die meisten vergessenen Zugänge entstehen nicht aus Bosheit, sondern weil niemand wusste, dass es sie gibt. Deshalb beginnt Offboarding mit einer Liste – idealerweise schon beim Onboarding.

- [ ] Zugangsliste der Person erstellen oder prüfen (Tabelle auf Seite 4): alle Konten, Geräte, Schlüssel, Vollmachten
  Auch das, was „nur kurz“ eingerichtet wurde: Testkonten, Kundenportale, Lieferantenshops
- [ ] Welche Zugänge sind geteilt? (Social-Media-Konto, Info-Postfach, WLAN, Alarmanlage, Lieferantenportal)
  Geteilte Passwörter müssen am letzten Tag geändert werden
- [ ] Wer übernimmt Kunden, Projekte, Postfach und Kalender? Übergabe terminieren
- [ ] Weiterleitungsregeln und App-Freigaben im Konto der Person prüfen
  Private Weiterleitungen an Gmail und Co. sind der häufigste unbemerkte Datenabfluss
- [ ] Geschäftsführung / Buchhaltung: Bank-Zeichnungsrechte, Kreditkarten, Zahlungsfreigaben, Firmenbuch-Vollmachten identifizieren
- [ ] Rückgabetermin für Geräte, Schlüssel, Zutrittskarten, Firmenhandy und SIM vereinbaren
- [ ] Bei Administratoren oder Schlüsselpersonen: zweite Admin-Person sicherstellen, bevor das Konto gesperrt wird
  Sonst sperren Sie sich selbst aus Microsoft 365, Hosting oder Domain aus

2 Am letzten Tag – in dieser Reihenfolge

- [ ] Microsoft 365 / Google Workspace: Konto sperren (nicht löschen), alle Sitzungen beenden, MFA-Geräte und App-Passwörter entfernen
  Microsoft: Benutzer → Anmeldung blockieren → Alle Sitzungen abmelden. Google: Benutzer sperren → Sitzungen zurücksetzen
- [ ] E-Mail: Weiterleitung an die übernehmende Person oder Autoantwort einrichten; Postfach in freigegebenes Postfach umwandeln
  Lizenz wird damit meist frei
- [ ] Passwort-Manager: Person aus dem Firmentresor entfernen, geteilte Einträge markieren

- [ ] Alle geteilten Passwörter ändern: WLAN, Info-Postfach, Social Media, Alarmanlage, Lieferanten- und Kundenportale, Steuerportale
- [ ] Website und Hosting: WordPress-Benutzer entfernen oder Rolle auf „Abonnent“, Hosting-/cPanel-Zugang, FTP, Domain-Registrar prüfen
  Zweitadmin bei der Agentur? Dann auch dort fragen
- [ ] Cloud- und Fachsoftware: Buchhaltung, CRM, Kalkulation, Zeiterfassung, Dropbox/OneDrive-Freigaben, Branchensoftware, Fernwartungstools
- [ ] VPN, Fernzugänge und Remote-Desktop: Zertifikate und Benutzer löschen; bei Steuerungen beim Kunden: Zugang entziehen
- [ ] Bank und Zahlungen: Online-Banking-Benutzer, Firmenkreditkarte, PayPal/Stripe, Zeichnungsrechte widerrufen
- [ ] Geräte zurück: Laptop, Handy, SIM, Token, USB-Sticks – Gerät aus der Ferne löschen, falls nicht zurückgegeben
  Vor der Neuvergabe: zurücksetzen, nicht nur „Benutzer löschen“
- [ ] Schlüssel, Zutrittskarten, Alarmcodes zurück bzw. Codes ändern
- [ ] Telefon: Rufumleitungen, Durchwahl, Firmenhandy-Nummer, Messenger-Gruppen (WhatsApp/Signal/Teams)

3 In den Tagen danach

- [ ] Anmeldeversuche auf das gesperrte Konto und die geänderten Zugänge eine Woche lang beobachten
  Microsoft 365: Anmeldeprotokolle; WordPress: Sicherheits-Plugin oder Xcubitor-Überwachung
- [ ] Lizenzen freigeben (Microsoft 365, Adobe, Fachsoftware) – spart Geld und schließt Türen
- [ ] Daten der Person archivieren: Postfach und Dateien nach DSGVO-Grundsätzen aufbewahren, Zugriff nur für Berechtigte
  Privates im Postfach? Nicht durchsuchen, sondern mit Rechtsberatung klären
- [ ] Kunden und Lieferanten über die neue Ansprechperson informieren – und darüber, dass die alte Adresse nicht mehr gilt
  Verhindert, dass Betrüger die alte Adresse nachahmen
- [ ] Dokumentation abschließen: Tabelle auf Seite 4 unterschreiben und ablegen (Nachweis für Versicherung, Audit, NIS2-Fragebogen)
- [ ] Nach 30 Tagen: Konto endgültig löschen, Postfach-Weiterleitung beenden, Archiv prüfen

4 Sonderfälle

Unfreiwilliges Ausscheiden / Konflikt

1. Konten sperren, **bevor** das Gespräch stattfindet – nicht danach.
2. Geräte und Schlüssel im Gespräch übernehmen; Fernlöschung vorbereiten.
3. Alle geteilten Passwörter noch am selben Tag ändern, Bank zuerst.
4. Zugriffsprotokolle der letzten 30 Tage sichern (Downloads, Weiterleitungen, Freigaben).

Administrator oder IT-Dienstleister

1. Globale-Admin-Rechte zuerst auf eine verbleibende Person übertragen, Notfall-Admin-Konto prüfen.
2. Alle Admin-Passwörter ändern: Microsoft 365, Hosting, Domain, Router, Firewall, Backup-System, Fernwartungstools.
3. API-Schlüssel, Dienstkonten und Automatisierungen prüfen, die auf die Person liefen.
4. Backups auf Zugriff und Vollständigkeit testen.

Lehrling, Praktikum, Aushilfe

1. Gleiche Liste, kürzere Version – kleine Konten sind genauso Einfallstor.
2. Geteilte Logins („Kassa“, „Werkstatt“) ändern.
3. Zugang zu WhatsApp-Gruppen und Social Media entfernen.

Agentur oder Dienstleister endet

1. Eigene Admin-Zugänge zu Website, Hosting, Domain, Analytics, Werbekonten sicherstellen – **Sie** müssen Eigentümer sein.
2. Zugänge des Dienstleisters entfernen, Passwörter und API-Schlüssel ändern.
3. Verträge, DSGVO-Auftragsverarbeitung und Datenrückgabe abschließen.

Warum das wichtig ist: Ein vergessener Zugang ist für Angreifer wie ein Ersatzschlüssel unter der Fußmatte. Beim Binance-Hack 2026 reichte ein einziges Gerät mit zu vielen Rechten für 6,3 Milliarden US-Dollar Schaden – in einem KMU reicht ein alter Hosting-Zugang für eine gehackte Website. Fallstudie: xcubitor.at/fallstudien/binance-hack-admin-laptop/

5 Zugangs- und Geräteliste

Eine Zeile pro Konto, Gerät oder Vollmacht. Beim Eintritt anlegen, beim Austritt abhaken – dann dauert Offboarding eine Stunde statt einer Woche.

✓	DIENST / GERÄT / VOLLMACHT	KONTO / NUMMER	ENTZOGEN AM	DURCH
☐	Microsoft 365 / Google Workspace			
☐	Passwort-Manager (Firmentresor)			
☐	WordPress / Website-Admin			
☐	Hosting / cPanel / FTP			
☐	Domain-Registrar / DNS			
☐	Buchhaltung / Fakturierung			
☐	CRM / Kundendatenbank			
☐	Branchensoftware / Kalkulation			
☐	Cloud-Speicher und Freigaben			
☐	VPN / Fernzugang / Fernwartung			
☐	Online-Banking, Kreditkarte, PayPal/Stripe			
☐	Social Media / Werbekonten (Admin)			
☐	WLAN-Passwort			
☐	Schlüssel, Zutrittskarte, Alarmcodes			
☐	Laptop, Handy, SIM (Seriennummern)			
☐	Messenger-Gruppen (WhatsApp, Teams)			
☐	Lieferanten- / Kundenportale			
☐	Behördenportale (FinanzOnline, USP)			

Ausscheidende Person, letzter Arbeitstag	
Abgeschlossen am / durch (Unterschrift)	

Ausführlicher Ratgeber zum IT-Offboarding erscheint am 18.11.2026 auf xcubitor.at/ratgeber/ · Microsoft-365-Anleitung: xcubitor.at/ratgeber/microsoft-365-absichern/ · Allgemeine Information, keine Rechtsberatung.

Sicherheit, die Ihnen erklärt wird

Xcubitor überwacht Website und Webhosting Ihres Unternehmens rund um die Uhr und warnt Sie in verständlicher Sprache. Zum Start prüfen wir, ob niemand mehr drin ist.

xcubitor.at/preise