

Regeln für sichere Konten

Anpassbare Vorlage für Mitarbeitende und IT. Vereinbaren Sie, wie Konten geschützt, wiederhergestellt und beendet werden. Vor Einführung an Ihre Systeme, Zuständigkeiten und internen Vorgaben anpassen.

Unternehmen / Geltungsbereich: _____

Verantwortlich / freigegeben am / nächste Prüfung: _____

Eigene Konten verwenden

Persönliche Konten nicht weitergeben. Berechtigungen auf die benötigte Aufgabe begrenzen.
Administrationskonten von der täglichen Arbeit trennen.

Passwörter sicher verwalten

Für jeden Dienst ein eigenes langes Passwort verwenden und mit dem freigegebenen Passwortmanager erzeugen und speichern. Masterpasswort und Wiederherstellung passend absichern.

MFA passend einrichten

Mit IT starke Mehrfaktor-Authentisierung einrichten. Wo unterstützt, phishingresistente Verfahren wie passend konfigurierte FIDO2-Passkeys oder Sicherheitsschlüssel mit PIN oder Biometrie bevorzugen.

Anmeldeanfragen bewusst prüfen

Nur selbst ausgelöste, zum eigenen Anmeldevorgang passende Anfragen bestätigen. Unerwartete Anfragen ablehnen und melden. Passwort, Einmalcode und Wiederherstellungscode nicht an Anrufende weitergeben.

Wiederherstellung vorbereiten

Ersatzfaktor und genehmigten Wiederherstellungsweg vorab klären. Codes geschützt nach interner Vorgabe aufbewahren, nicht ausschließlich hinter dem gesperrten Konto. Keine Codes in diese Vorlage eintragen.

Änderungen und Verdacht melden

Verlust eines Geräts, verdächtige Anmeldungen und nicht mehr benötigte Rechte zeitnah melden. Bei Verdacht koordiniert IT auch die Prüfung aktiver Sitzungen, Faktoren und App-Zugriffe.

Interne Anlaufstellen

Freigegebener Passwortmanager / interne Anleitung: _____

IT-Kontakt / Ersatzkontakt bei Kontosperre: _____

Ablage der Wiederherstellungsanleitung ohne Codes: _____

Checkliste zur Kontowiederherstellung

Nur das abgestimmte Verfahren für eigene oder ausdrücklich zur Betreuung freigegebene Konten verwenden. Zuständige IT einbeziehen; diese Vorlage ist keine Berechtigung zur Kontoübernahme.

Betroffener Dienst / interner Vorgang / Zeitpunkt: _____

Erreichbarer Kontakt / geprüft durch: _____

Situation unterscheiden

Gerät verloren, Faktor defekt oder verdächtige Anmeldung? Bei Verdacht sofort den internen Vorfallweg nutzen; ein Passwortwechsel allein genügt möglicherweise nicht.

Bekannten Kontakt nutzen

IT über die hinterlegte Nummer oder das bekannte Portal erreichen. Keine Hilfe über ungeprüfte Suchanzeigen, fremde Rückrufnummern oder unerwartete Links anfordern.

Identität prüfen lassen

Das vereinbarte Prüfverfahren mit IT durchführen. Dringlichkeit ist kein Ersatz für Identitätsprüfung. Keine MFA-Codes an Anrufende übermitteln.

Freigegebenen Ersatzweg nutzen

Ersatzfaktor oder geschützte Wiederherstellung nach interner Freigabe einsetzen. Verlorene Faktoren sperren und neue Faktoren kontrolliert registrieren lassen.

Bei Verdacht weitere Zugriffe prüfen

IT prüft unter anderem aktive Sitzungen, Tokens, App-Freigaben, Wiederherstellungsdaten und Postfachregeln. Betroffene Zugriffe nach Lage sperren oder widerrufen.

Abschluss dokumentieren

Erreichbarkeit und Anmeldung testen, Ersatzweg aktualisieren und Maßnahmen im internen Vorgang festhalten. Keine Geheimnisse in das Protokoll kopieren.

Maßnahmen / zuständig / abgeschlossen am: _____

Ergebnis des Anmeldetests / nächste Prüfung: _____

Zugänge vergeben ändern und entziehen

Für Eintritt, Rollenwechsel und Austritt. Personalverantwortliche, Fachbereich und IT legen Freigabe, Umsetzung und Kontrolltermin fest. Für zusätzliche Dienste weitere Zeilen ergänzen.

Person oder interne Referenz / Rolle: _____
Anlass / wirksam ab / freigegeben durch: _____

Dienst oder Konto	Benötigte Rechte und Aktion	Umsetzung und Beleg
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____
_____	_____	_____

Bei Eintritt und Rollenwechsel

Identität und Freigabe prüfen, nur erforderliche Rechte einrichten, MFA und Wiederherstellung vorbereiten. Beim Wechsel alte Rechte ausdrücklich entfernen. Befristung und nächste Prüfung dokumentieren; administrative Rechte separat freigeben.

Beim Austritt

Zum freigegebenen Zeitpunkt Konten und Fernzugänge sperren, Sitzungen und Tokens widerrufen und MFA-Faktoren prüfen. Auch Dienste außerhalb des zentralen Logins berücksichtigen. Geräte, Schlüssel und gemeinsame Geheimnisse prüfen; betroffene gemeinsame Geheimnisse erneuern. Daten und Verantwortlichkeiten nach internen Vorgaben übergeben. Löschungen und Aufbewahrung gesondert klären.

Abschlusskontrolle durch / Datum / offene Punkte: _____

Nutzung und Quellen

Eigene Vorlagen der Paragamix GmbH. Kostenlos intern nutzen, anpassen und an Kunden weitergeben. Quellenlink willkommen, aber nicht erforderlich. Keine vollständige Berechtigungsprüfung oder Konformitätsbestätigung. Keine Passwörter, Tokens oder Wiederherstellungscodes eintragen.

[NCSC Identity and access](#) | [NCSC MFA](#) | [NCSC Password managers](#)

[Aktuelle Fassung und Praxisfälle](#)