Eintritt, Wechsel und Austritt

Für Personalabteilung, Abteilungsleitungen und alle, die die Systeme verwalten: wer entscheidet, wer setzt um und wer hält fest, bei jedem Menschen, der kommt, wechselt oder geht.

Kategorie: Arbeitsblatt. Bezug im Buch: Abschnitt 2.1 (Leitfrage, Tabellen 1, 2, 4 und 5); Norm: Maßnahmen A 5.11, 5.15 bis 5.18, 6.5, 8.2, 8.3, 8.5, 8.15 und 8.16 der ISO/IEC 27001:2022 mit Änderung 1:2024, in den eigenen Worten des Bandes. Rechtsstand des Bandes: 27. September 2026.

Haus		**Stand (Datum)**	
Ausgefüllt von (Personalabteilung)		**Ausgefüllt von (Systemverwaltung)**	

So nutzen Sie diese Vorlage

1. Lassen Sie sich die Liste aller Konten des Hotelverwaltungssystems geben und legen Sie sie neben die Lohnabrechnung dieses Monats. Zählen Sie die Namen, die auf der ersten Liste stehen und auf der zweiten nicht (Teil 1). Jedes dieser Konten gehört einem Menschen, den das Haus nicht mehr beschäftigt und dem es nichts mehr anweisen kann.
2. Bei jedem der drei Ereignisse (Teil 2) entscheidet eine benannte Person im Betrieb, welcher Zugang gebraucht wird; jemand anderes setzt ihn um und hält ihn fest. Tragen Sie die Namen ein, nicht die Abteilungen.
3. Die Abteilungsleitungen prüfen ihre Konten einige Male im Jahr (Teil 3): Wer weiß, ob ein Zugang richtig ist, ist die Leitung der Abteilung, nicht die IT.

Spalte «Im Buch»: verlangt = von der Norm verlangt, wie der Band sie in eigenen Worten wiedergibt (Maßnahme in Klammern); Methode = Vorgehen dieses Bandes, keine Anforderung.

1 Die Kontenliste neben der Lohnabrechnung

Befund	Unser Haus	Grund (aus dem Band)	Im Buch	Beispiel Augsburg
Aktive Konten im Verwaltungssystem, und Beschäftigte laut Lohnabrechnung	Konten: _____ Beschäftigte: _____	In einem Hotel wechseln die Menschen schneller als die Systeme; die Konten entfernen sich jeden Monat weiter von den Menschen, die es beschäftigt.	**Methode** dieses Bandes: die Gegenüberstellung der beiden Listen, für jedes System des Hauses.	168 Konten für 110 Beschäftigte
Konten von Menschen, die gegangen sind		Die Befugnis endet mit dem Arbeitsverhältnis, nicht mit dem Konto.	**verlangt:** Zugriffsrechte entzogen (A 5.18); Pflichten und Rückgabe beim Austritt (A 6.5, 5.11).	29, eines für die Stornierungen benutzt
Konten, die sich mehrere Menschen teilen		Jede Handlung ließ sich niemandem zuordnen; die Protokolle hätten auf alle gezeigt, und damit auf niemanden.	**Methode** dieses Bandes.	1 Konto, 7 Menschen
Konten von Lieferanten und Dienstleistern, die niemand zuordnen kann		Zwölf Konten gehörten Lieferanten und Dienstleistern, von denen einige niemand zuordnen konnte.	**verlangt:** Lebenszyklus der Identitäten verwaltet (A 5.16).	12, mehrere niemandem zuzuordnen
Beschäftigte mit Rechten aus früheren Stellen		Jeder Wechsel fügte Rechte hinzu und entfernte keine; so entstanden Kombinationen wie Belastungen buchen und Erstattungen genehmigen.	**verlangt:** Zugriffsrechte geändert (A 5.18).	etwa 14
Alarm bei ungewöhnlicher Anmeldung eingeschaltet, und wer ihn liest	☐ ja ☐ nein Gelesen von: _____	Das Verwaltungssystem zeichnete jede Anmeldung auf; niemand sah die Aufzeichnungen an, bis etwas schiefgegangen war.	**verlangt:** Protokolle ausgewertet (A 8.15), Netze und Systeme auf ungewöhnliches Verhalten überwacht (A 8.16).	0: Funktion vorhanden, abgeschaltet

Spalte «Beispiel Augsburg»: **Beispiel aus Abschnitt 2.1** (Tabelle 1), Illustration, nicht Ihre Antwort. Das Ergebnis kostete zwei Tage Arbeit und erforderte keine Werkzeuge, die das Haus nicht besaß.

2 Drei Ereignisse, eine Regel: die Fragen

Nr.	Frage	Grund (aus dem Band)	Im Buch	Wer entscheidet · wer setzt um und hält fest
E1	**Eintritt:** Welche Rolle hat dieser Mensch, und wer in der Abteilungsleitung fordert die Rechte dieser Rolle an?	Das kopierte Konto trug alles, was seine ursprüngliche Inhaberin im Lauf der Jahre angesammelt hatte.	**verlangt:** Regeln für den Zugang nach den Anforderungen (A 5.15); Rechte kommen aus der Rolle, nicht aus dem Menschen (A 5.15, 8.3).	
E2	**Eintritt:** Sind die Rechte der Rolle vergeben, bevor die erste Schicht beginnt?	Das Konto wurde meist am Morgen des ersten Arbeitstages angefordert; niemand entschied, was genau dieser Mensch braucht.	**verlangt:** Zugriffsrechte nach Richtlinie vergeben (A 5.18). **Methode:** vor der ersten Schicht.	
W1	**Wechsel:** Was braucht die neue Stelle, was nicht mehr die alte, und wer entscheidet das?	Hotels befördern aus den eigenen Reihen; jeder Wechsel fügte Rechte hinzu und entfernte keine.	**verlangt:** Zugriffsrechte geändert (A 5.18).	
W2	**Wechsel:** Sind die Rechte der alten Rolle am selben Tag entfernt, auch bei Auszubildenden, die planmäßig Empfang, Reservierung, Service, Etage, Küche und Verwaltung durchlaufen?	Nach einigen Jahren hielten die Beschäftigten mit den abwechslungsreichsten Laufbahnen den breitesten Zugang im Haus.	**verlangt:** Zugriffsrechte entzogen (A 5.18). **Methode:** am selben Tag.	

Nr.	Frage	Grund (aus dem Band)	Im Buch	Wer entscheidet · wer setzt um und hält fest
A1	**Austritt:** Welche Konten hat dieser Mensch, in welchem System auch, und wer liefert es?	Die Schlüssel zum Gebäude wurden am letzten Tag zurückgegeben; der Schlüssel zum System, der weit mehr öffnete, blieb bei dem, der gegangen war.	**verlangt:** Rückgabe von Werten, zu denen der Zugang gehört (A 5.11); Lebenszyklus der Identitäten (A 5.16).	
A2	**Austritt:** Benachrichtigt der Austrittsablauf der Personalabteilung die Stelle, die die Systeme verwaltet, und wie?	Der Austrittsablauf der Personalabteilung war sorgfältig; nichts darin benachrichtigte die IT.	**verlangt:** Lebenszyklus über einen Ablauf, der jedes System erreicht (A 5.16).	
A3	**Austritt:** Sind alle Konten am letzten Arbeitstag geschlossen, für alle, nicht nur im Streit?	Eine Routine, die für alle gilt, kränkt niemanden; eine Sperre, die nur im Streit verhängt wird, kommt meist zu spät.	**verlangt:** Zugriffsrechte entzogen (A 5.18); Pflichten nach der Beschäftigung (A 6.5). **Methode:** die Routine für alle.	

3 Dazu: Überprüfung, Administratoren, Anmeldung, Alarm

Nr.	Frage	Grund (aus dem Band)	Im Buch	Eintrag
P1	Prüft jede Abteilungsleitung einige Male im Jahr die Konten ihrer Leute und unterschreibt die Liste: Arbeitet jeder noch hier, und braucht jeder noch, was er hat?	Die IT konnte die Konten sehen; nur die Abteilungen konnten sehen, ob sie stimmten.	**verlangt:** Zugriffsrechte überprüft (A 5.18). Die Norm schreibt nicht vor, wie oft; das Haus legt es fest und belegt es. Quartal und Unterschrift: möglicher Nachweis.	
P2	Gibt es eine Liste der Administratorkonten, jedes benannt, jedes mit zweitem Faktor?	Privilegierte Rechte sind zu beschränken: wenige, benannte Administratoren.	**verlangt:** privilegierte Zugriffsrechte beschränkt und verwaltet (A 8.2).	
P3	Haben die Systeme, die von außerhalb des Hauses erreichbar sind, einen zweiten Faktor?	Das Verwaltungssystem war aus jedem Browser der Welt erreichbar; der Zugang endete erst, wenn das Konto endete.	**verlangt:** sichere Authentisierung nach der Empfindlichkeit der Information (A 8.5).	
P4	Meldet ein Alarm Anmeldungen zu ungewöhnlicher Stunde oder von außen, und liest ihn eine benannte Person?	Der Beweis lag seit dem Weggang offen da, eine Anmeldung um drei Uhr morgens mit einem elf Wochen nicht benutzten Konto.	**verlangt:** A 8.15, 8.16. Der Alarm in dieser Form: Methode; die Auswertung des Beschäftigtenverhaltens berührt die Mitbestimmung (Abschnitt 2.14).	

Abteilung	Leitung	Geprüft am	Konten gesehen	zu schließen / zu ändern	Unterschrift

4 Was das Recht zum offenen Konto sagt

Ebene	Deutschland	Österreich	Schweiz
Unbefugter Zugang	Ausspähen von Daten (StGB § 202a); ein Passwort gilt als Zugangssicherung	widerrechtlicher Zugriff auf ein Computersystem, mit besonderem Vorsatz (StGB § 118a)	unbefugtes Eindringen in ein besonders gesichertes Datenverarbeitungssystem (StGB Art. 143bis)
Meldung des Hauses	Aufsichtsbehörde binnen 72 Stunden, außer bei voraussichtlich keinem Risiko (Art. 33 DSGVO)	ebenso, an die Datenschutzbehörde	EDÖB, wenn voraussichtlich ein hohes Risiko besteht (revDSG Art. 24)

Die Befugnis endet mit dem Arbeitsverhältnis, nicht mit dem Konto. Dieselben Protokolle, die einen früheren Mitarbeiter überführen, zeigen der Aufsichtsbehörde, dass das Haus ihm den Zugang gelassen hatte: Das Haus sollte die Maßnahmen, die es danach ergriffen hat, ordnen können, wenn die Behörde fragt. Auch ohne kopierte Daten kann die Stornierung von Reservierungen durch einen Unbefugten eine Verletzung der Integrität und Verfügbarkeit personenbezogener Daten sein; wer auf eine Meldung verzichtet, sollte gute Gründe schriftlich haben.

Was diese Vorlage nicht ist

Dieses Blatt ersetzt weder die Norm noch eine Rechtsberatung noch die Auskunft von Betriebsrat oder Aufsichtsbehörde und ist kein Nachweis: Ein ausgefülltes Blatt belegt weder einen geschlossenen Zugang noch eine geprüfte Kontenliste; das tun nur die Konten selbst und die unterschriebenen Listen der Abteilungen. Die Fragen in dieser Form sind Methode dieses Bandes, keine Anforderung; verlangt ist, was mit einer Maßnahme des Anhangs A gekennzeichnet ist. Die Angaben zum Recht geben den Stand des Bandes wieder (Rechtsstand des Bandes: 27. September 2026).