5 Reduktion von Zugriffen auf Dateien und Programmen auf das erforderliche Ausmaß

Die Zugriffsrechte zu Anwendungen und zu Dateisystemen sind geregelt. Die gesetzten Berechtigungen stellen sicher, dass nur die Personen zugreifen können, die aufgrund ihrer Tätigkeit einen Bedarf dafür haben (Need-to-know-Prinzip). Die Berechtigungen sind auf das notwendige Ausmaß begrenzt.

Quelle Ziffern 1,6,7:

Leitfaden technische und organisatorische Maßnahmen DSGVO (WKÖ)

<https://www.wko.at/oe/it-sicherheit/leitfaden-massnahmen-dsgvo-1.pdf>

Quelle Ziffern 2-4:

BSI IT-Grundschutz-Bausteine Organisation und Personal (ORP 4); 2023

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/02_ORP_Organisation_und_Personal/ORP_4_Identitaets_und_Berechtigungsmanagement_Editon_2023.pdf?__blob=publicationFile&v=3#download=1>

[1. User-Management 1](#_Toc144815456)

[2. Einrichtung von Benutzenden und Benutzendengruppen 1](#_Toc144815457)

[3. Einrichtung, Änderung und Entzug von Berechtigungen 2](#_Toc144815458)

[4. Dokumentation der Benutzendenkennung und Rechteprofile 2](#_Toc144815459)

[5. Vergabe von Zugriffsrechten. 2](#_Toc144815460)

[6. Regelung für den Einsatz von Fremdpersonal 2](#_Toc144815461)

[7. Verfahren bei personellen Veränderungen 3](#_Toc144815462)

[8. Weiterführendes/Normen 3](#_Toc144815463)

# User-Management

Die Verwaltung von Benutzern stellt einen kritischen Bereich dar. Durch die Erstellung von Benutzerprofilen sollte genau geregelt werden, wer auf welche Daten zugreifen darf und auch das Recht hat, diese zu verändern oder zu löschen.

Administratoren, die diese Aufgaben erfüllen, sind entsprechend zu schulen und müssen auch nachweislich den vorgegebenen organisatorischen Regeln folgen. Dazu gehört vor allem die revisionssichere Protokollierung bei der Einrichtung von Benutzern.

Grundsätzlich dürfen nur berechtigte Personen Zugriffe auf personenbezogene Daten durchführen.

# Einrichtung von Benutzenden und Benutzendengruppen

Es MUSS geregelt werden, wie Benutzendenkennungen und -gruppen einzurichten und zu löschen sind. Jede Benutzendenkennung MUSS eindeutig einer Person zugeordnet werden können.

Benutzendenkennungen, die längere Zeit inaktiv sind, SOLLTEN deaktiviert werden. Alle Benutzenden und Benutzendengruppen DÜRFEN NUR über separate administrative Rollen eingerichtet und gelöscht werden. Nicht benötigte Benutzendenkennungen, wie z. B. standardmäßig eingerichtete Gastkonten oder Standard-Administrierendenkennungen, MÜSSEN geeignet deaktiviert oder gelöscht werden.

# Einrichtung, Änderung und Entzug von Berechtigungen

Benutzendenkennungen und Berechtigungen DÜRFEN NUR aufgrund des tatsächlichen Bedarfs und der Notwendigkeit zur Aufgabenerfüllung vergeben werden (Prinzip der geringsten Berechtigungen, englisch principle of least privilege, und Erforderlichkeitsprinzip, englisch need-to-know principle). Bei personellen Veränderungen MÜSSEN die nicht mehr benötigten Benutzendenkennungen und Berechtigungen entfernt werden. Beantragen Mitarbeitende Berechtigungen, die über den Standard hinausgehen, DÜRFEN diese NUR nach zusätzlicher Begründung und Prüfung vergeben werden.

Zugriffsberechtigungen auf Systemverzeichnisse und -dateien SOLLTEN restriktiv eingeschränkt werden. Alle Berechtigungen MÜSSEN über separate administrative Rollen eingerichtet werden.

# Dokumentation der Benutzendenkennung und Rechteprofile

Es MUSS dokumentiert werden, welche Benutzendenkennungen, Benutzendengruppen und Rechteprofile zugelassen und angelegt wurden. Die Dokumentation der zugelassenen Benutzendenkennungen sowie angelegten Benutzendengruppen und Rechteprofile MUSS regelmäßig daraufhin überprüft werden, ob sie den tatsächlichen Stand der Rechtevergabe widerspiegelt. Dabei MUSS auch geprüft werden, ob die Rechtevergabe noch den Sicherheitsanforderungen und den aktuellen Aufgaben der Benutzenden entspricht. Die Dokumentation MUSS vor unberechtigtem Zugriff geschützt werden. Sofern sie in elektronischer Form erfolgt, SOLLTE sie in das Datensicherungsverfahren einbezogen werden.

# Vergabe von Zugriffsrechten

Es MUSS festgelegt werden, welche Zugriffsrechte an welche Personen im Rahmen ihrer Funktion vergeben bzw. ihnen entzogen werden. Werden im Rahmen der Zugriffskontrolle Chipkarten oder Token verwendet, so MUSS die Ausgabe bzw. der Entzug dokumentiert werden. Die Anwendenden SOLLTEN für den korrekten Umgang mit Chipkarten oder Token geschult werden. Bei längeren Abwesenheiten SOLLTEN berechtigte Personen vorübergehend gesperrt werden.

# Regelung für den Einsatz von Fremdpersonal

Betriebsfremde Personen wie z.B. Personal von Reinigungsfirmen oder IT-Dienstleister können leicht Zugang zu vertraulichen Unternehmensdaten erhalten und stellen unter Umständen eine erhebliche Bedrohung dar.

Einige einfache Regeln sollten beachtet werden, um vertrauliche Informationen zu schützen:

* Externe Mitarbeiterinnen und Mitarbeiter, die über einen längeren Zeitraum in einem Unternehmen tätig sind und Zugang zu vertraulichen Unterlagen und Daten erhalten könnten, müssen schriftlich (im Rahmen von Geheimhaltungsverpflichtungen) auf die Einhaltung der geltenden einschlägigen Gesetze, Vorschriften und internen Regelungen verpflichtet werden.
* Für Fremdpersonal, das nur kurzfristig oder einmalig zum Einsatz kommt, gelten die gleichen Regeln wie für Besucherinnen und Besucher, d.h. dass etwa der Aufenthalt in sicherheitsrelevanten Bereichen nur in Begleitung von unternehmenseigenem Personal erlaubt ist.
* Ist es nicht möglich, betriebsfremde Personen ständig zu begleiten oder zu beaufsichtigen, sollten zumindest die persönlichen Arbeitsbereiche abgeschlossen werden (Schreibtisch, Schrank, Abmeldung/Sperre am PC).

# Verfahren bei personellen Veränderungen

Bei personellen Veränderungen, insbesondere beim Ausscheiden von Mitarbeiterinnen und Mitarbeitern aus dem Unternehmen, sollten folgende grundlegende Punkte beachtet werden:

* Sämtliche Unterlagen, ausgehändigte Schlüssel und zur Verfügung gestellte IT-Geräte (z.B. Mobilgeräte, Speichermedien, Dokumentationen) sind zurückzufordern.
* Sämtliche Zugangsberechtigungen und Zugriffsrechte müssen angepasst, entzogen oder gelöscht werden. Dies betrifft unter anderem auch Berechtigungen für eventuelle Telearbeitszugänge sowie Daten auf privaten Smartphones oder Notebooks.
* Wenn eine Zugangsberechtigung zu einem IT-System zwischen mehreren Personen geteilt wurde (z.B. mittels eines gemeinsamen Passwortes), muss nach Ausscheiden einer der Personen die Zugangsberechtigung sofort geändert werden. Wenn Administratoren oder andere Schlüsselpersonen ausscheiden, müssen auch alle anderen Passwörter geändert werden, die ihnen bekannt waren.
* Die Neuvergabe eines bestehenden Benutzerkontos an neue Mitarbeiterinnen oder Mitarbeiter sollte möglichst vermieden werden.

Es empfiehlt sich eine Checkliste für personelle Veränderungen bereitzuhalten.

# Weiterführendes/Normen

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 27001:2013 „Information technology – Security techniques – Information security management systems – Requirements“ im Anhang A.9 Zugangssteuerung Vorgaben für das Identitäts- und Berechtigungsmanagement.

Die International Organization for Standardization (ISO) gibt in der Norm ISO/IEC 29146:2016 „Information technology – Security techniques – A framework for access management“ Vorgaben für das Identitäts- und Berechtigungsmanagement.

Das Information Security Forum (ISF) macht in seinem Standard „The Standard of Good Practice for Information Security“ im Kapitel TS1.4 Identity and Access Management Vorgaben für das Identitäts- und Berechtigungsmanagement.

Das National Institute of Standards and Technology (NIST) gibt in der NIST Special Publication 800- 53A, insbesondere Bereiche AC und IA, Hinweise für Identitäts- und Berechtigungsmanagement.

Dieses Dokument wurden von einer Expertengruppe der Cybersicherheit-Plattform (CSP) erstellt.

Alle Angaben erfolgen trotz sorgfältigster Bearbeitung ohne Gewähr. Eine Haftung der Wirtschaftskammern Österreichs, der CSP oder der Mitglieder der Expertengruppe ist ausgeschlossen.

Bei allen personenbezogenen Bezeichnungen gilt die gewählte Form für alle Geschlechter!

Stand: März 2024