|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Sicherheitsrichtlinie "Identitäts- und Berechtigungsmanagement"

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300008 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc146184160)

[Dokumentenhistorie 3](#_Toc146184161)

[Inhaltsverzeichnis 4](#_Toc146184162)

[Allgemeine Festlegungen 6](#_Toc146184163)

[Ziel / Zweck 6](#_Toc146184164)

[Geltungsbereich 6](#_Toc146184165)

[Zuständigkeiten 7](#_Toc146184166)

[Genehmigungs- und Änderungsverfahren 7](#_Toc146184167)

[Aufbau des Dokuments 7](#_Toc146184168)

[Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagement" 8](#_Toc146184169)

[Basismaßnahmen 8](#_Toc146184170)

[Regelung für die Einrichtung von Benutzern und Benutzergruppen (ORP.4.A1) 8](#_Toc146184171)

[Regelung für Einrichtung, Änderung und Entzug von Berechtigungen (ORP.4.A2) 8](#_Toc146184172)

[Dokumentation der Benutzerkennungen und Rechteprofile (ORP.4.A3) 8](#_Toc146184173)

[Aufgabenverteilung und Funktionstrennung (ORP.4.A4) 8](#_Toc146184174)

[Vergabe von Zutrittsberechtigungen (ORP.4.A5) 8](#_Toc146184175)

[Vergabe von Zugangsberechtigungen (ORP.4.A6) 9](#_Toc146184176)

[Vergabe von Zugriffsrechten (ORP.4.A7) 9](#_Toc146184177)

[Regelung des Passwortgebrauchs (ORP.4.A8) 9](#_Toc146184178)

[Identifikation und Authentisierung (ORP.4.A9) 10](#_Toc146184179)

[Regelung zur Passwortqualität (ORP.4.A22) 10](#_Toc146184180)

[Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme (ORP.4.A23) 10](#_Toc146184181)

[Standardmaßnahmen 10](#_Toc146184182)

[Schutz von Benutzerkennungen mit weitreichenden Berechtigungen (ORP.4.A10) 11](#_Toc146184183)

[Zurücksetzen von Passwörtern (ORP.4.A11) 11](#_Toc146184184)

[Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (ORP.4.A12) 11](#_Toc146184185)

[Geeignete Auswahl von Authentisierungsmechanismen (ORP.4.A13) 11](#_Toc146184186)

[Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung (ORP.4.A14) 11](#_Toc146184187)

[Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement (ORP.4.A15) 11](#_Toc146184188)

[Richtlinien für die Zugriffs- und Zugangskontrolle (ORP.4.A16) 12](#_Toc146184189)

[Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (ORP.4.A17) 12](#_Toc146184190)

[Einsatz eines zentralen Authentisierungsdienstes (ORP.4.A18) 12](#_Toc146184191)

[Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen (ORP.4.A19) 12](#_Toc146184192)

[Maßnahmen bei erhöhtem Schutzbedarf 12](#_Toc146184193)

[Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System (ORP.4.A20) 12](#_Toc146184194)

[Mehr-Faktor-Authentisierung (ORP.4.A21) 13](#_Toc146184195)

# Allgemeine Festlegungen

## Ziel / Zweck

Der Zugang zu schützenswerten Ressourcen der <Institution> ist auf berechtigte Benutzer (bspw. Mitarbeitende und Freelancer) und berechtigte IT-Komponenten einzuschränken. Benutzer und IT-Komponenten müssen zweifelsfrei identifiziert und authentisiert werden. Die Verwaltung der dafür notwendigen Informationen wird seitens der <Institution> als Identitätsmanagement bezeichnet.

Beim Berechtigungsmanagement der <Institution> geht es darum, ob und wie Benutzer oder IT-Komponenten auf Informationen oder Dienste zugreifen und diese benutzen dürfen. Benutzern wird also basierend auf dem Benutzerprofil Zutritt, Zugang oder Zugriff gewährt oder verweigert. Berechtigungsmanagement bezeichnet somit die Prozesse, die für die Zuweisung, den Entzug und die Kontrolle der Rechte erforderlich sind.

Die Übergänge zwischen den beiden Begriffen sind fließend, daher wird in dieser Sicherheitsrichtlinie der Begriff Identitäts- und Berechtigungsmanagement (englisch Identity and Access Management, IAM) benutzt. Zur besseren Verständlichkeit wird der Begriff "Benutzerkennung" bzw. "Kennung" synonym für "Benutzerkonto", "Login" und "Account" verwendet. In dieser Sicherheitsrichtlinie wird der Begriff "Passwort" als allgemeine Bezeichnung für "Passphrase", "PIN" oder "Kennwort" verwendet.

Ziel dieser Sicherheitsrichtlinie ist es, dass Benutzer oder auch IT-Komponenten ausschließlich auf die IT-Ressourcen und Informationen zugreifen können, die sie für ihre Arbeit benötigen und für die die Benutzer autorisiert sind, und nicht autorisierten Benutzern oder IT-Komponenten den Zugriff zu verwehren. Dazu werden Anforderungen formuliert, mit denen die <Institution> ein sicheres Identitäts- und Berechtigungsmanagement aufbauen kann. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Baustein ORP.4 "Identitäts- und Berechtigungsmanagement" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument "Sicherheitsrichtlinie Identitäts- und Berechtigungsmanagement“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Identitäts- und Berechtigungsmanagement"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Regelung für die Einrichtung von Benutzern und Benutzergruppen (ORP.4.A1)

Benutzer und Benutzergruppen sind ausschließlich von Personen mit administrativen Rechten über einen festgelegten Prozess einzurichten.

### Regelung für Einrichtung, Änderung und Entzug von Berechtigungen (ORP.4.A2)

Die Berechtigungen sind nach dem Need-to-Know-Prinzip zu vergeben. Sie werden nur zur Erfüllung der jeweiligen Aufgabe vergeben und sind bei Änderung des Aufgabenbereiches anzupassen.

Über den Standard hinausgehende Berechtigungen sind über den etablierten Prozess zu beantragen und freizugeben. Im Rahmen der Beantragung ist die Notwendigkeit der abweichenden bzw. erweiterten Berechtigung darzulegen.

### Dokumentation der Benutzerkennungen und Rechteprofile (ORP.4.A3)

Eine Dokumentation der zugelassenen Benutzer, der angelegten Benutzergruppen und der Rechteprofile ist zu erstellen. Die Dokumentation der zugelassenen Benutzer, der angelegten Benutzergruppen und der Rechteprofile ist regelmäßig auf Aktualität zu überprüfen. Die Dokumentation ist zu klassifizieren und vor unbefugtem Zugriff zu schützen. Soweit die Dokumentation in elektronischer Form erfolgt, ist sie in das etablierte Datensicherungsverfahren einzubeziehen.

Zur Vereinfachung der Dokumentationsaufgaben sind alle Benutzer- und Gruppenberechtigungen in einem zentralen System zu hinterlegen. Über dieses System kann eine regelmäßige Überprüfung erfolgen. Der Zugriff auf dieses System ist zu regeln und das System ist in die etablierten Prozesse der Datensicherung und -wiederherstellung einzubinden.

### Aufgabenverteilung und Funktionstrennung (ORP.4.A4)

Der Standard „IT-Administration“ dokumentiert, wie die Aufgaben der Administration aufgeteilt sind und welche Aufgaben unvereinbar sind.

### Vergabe von Zutrittsberechtigungen (ORP.4.A5)

Im Standard „Physische Sicherheit“ wird die Vergabe von Zutrittsberechtigungen dokumentiert.

Es gilt das Minimalprinzip. Der Zutritt richtet sich nur nach der Notwendigkeit zur Erfüllung der jeweiligen Aufgaben. Die Zutrittsberechtigungen werden zentral dokumentiert.

Bei der Vergabe von Zutrittsmedien ist zu dokumentieren, wer welche Medien erhalten hat und alle Nutzer sind im Umgang mit den Medien zu unterweisen.

Bei längerer vollständiger Abwesenheit eines Zutrittsberechtigten (z.B. Elternzeit, Sabbatical) sind die Zutrittsberechtigungen für diesen Zeitraum zu deaktivieren.

### Vergabe von Zugangsberechtigungen (ORP.4.A6)

Der Standard „IT-Administration“ dokumentiert, wie die Aufgaben der Administration verteilt sind und welche Aufgaben unvereinbar sind.

Es gilt das Minimalprinzip. Der Zugang richtet sich nur nach der Notwendigkeit zur Erfüllung der jeweiligen Aufgaben. Die Zugangsberechtigungen werden zentral dokumentiert.

Werden zur zusätzlichen Absicherung des Zugangs (MFA) Zugangsmittel wie z.B. USB-Keys ausgegeben, ist zu dokumentieren, wer welches Mittel erhalten hat und alle Nutzer sind im Umgang mit diesen Mitteln zu schulen.

Bei längerer Abwesenheit einer zugangsberechtigten Person (z.B. Elternzeit, Sabbatical) werden die Zugangsberechtigungen deaktiviert.

### Vergabe von Zugriffsrechten (ORP.4.A7)

Der Standard „IT-Administration“ dokumentiert, wie die Aufgaben der Administration aufgeteilt sind und welche Aufgaben unvereinbar sind.

Es gilt das Minimalprinzip. Der Zugriff richtet sich nur nach der Notwendigkeit zur Erfüllung der jeweiligen Aufgaben. Die Zugriffsrechte sind zentral dokumentiert.

Werden zur zusätzlichen Absicherung des Zugriffs (MFA) auf vertrauliche oder streng vertrauliche Informationen Zugriffsmittel wie z.B. USB-Keys ausgegeben, ist zu dokumentieren, wer welches Mittel erhalten hat und alle Benutzer sind im Umgang mit diesen Mitteln zu schulen.

Bei längerer Abwesenheit einer zugriffsberechtigten Person (z.B. Elternzeit, Sabbatical) sind die Zugriffsberechtigungen zu deaktivieren.

### Regelung des Passwortgebrauchs (ORP.4.A8)

Das Dokument "Umgang mit Passwörtern" regelt den Umgang mit Passwörtern.

Im Dokument "Umgang mit Passwörtern" werden die Passwortlänge, die Komplexität und die Häufigkeit des Passwortwechsels festgelegt. Diese Vorgaben sind als Validierung in den Systemen vorzugeben.

In Systemen vorinstallierte Standardpasswörter werden entsprechend dem Dokument "Umgang mit Passwörtern" geändert.

Passwörter werden unverzüglich geändert, sobald sie Unbefugten bekannt geworden sind oder der Verdacht besteht, dass sie Unbefugten bekannt geworden sind. Passwörter sind geheim zu halten. Im Rahmen der Nutzersensibilisierung wird darauf hingewiesen, dass Passwörter nicht mehrfach verwendet werden dürfen, um die Angriffsfläche für Zugänge und Zugriffe zu verringern.

Es wird sichergestellt, dass die mögliche Passwortlänge vom IT-System vollständig geprüft wird. Bei erfolglosen Anmeldeversuchen gibt das System keinen Hinweis darauf, dass das Passwort oder die Benutzerkennung falsch sind.

### Identifikation und Authentisierung (ORP.4.A9)

Der Zugang zu allen IT-Systemen und Diensten ist durch eine dem Schutzbedarf angemessene Identifizierung und Authentisierung der zugreifenden Benutzer, Dienste oder IT-Systeme gesichert. Vorkonfigurierte Zugänge werden vor dem produktiven Einsatz entsprechend angepasst.

### Regelung zur Passwortqualität (ORP.4.A22)

Das Dokument "Umgang mit Passwörtern" regelt den Umgang mit Passwörtern.

Im Dokument "Umgang mit Passwörtern" werden die Passwortlänge, die Komplexität und die Häufigkeit des Passwortwechsels festgelegt. Diese Vorgaben sind als Validierung in den Systemen vorzugeben.

In Systemen vorinstallierte Standardpasswörter werden entsprechend dem Dokument "Umgang mit Passwörtern" geändert.

### Regelung für Passwort-verarbeitende Anwendungen und IT-Systeme (ORP.4.A23)

Das Dokument "Umgang mit Passwörtern" regelt den Umgang mit Passwörtern.

Im Dokument "Umgang mit Passwörtern" werden die Passwortlänge, die Komplexität und die Häufigkeit des Passwortwechsels festgelegt. Diese Vorgaben sind als Validierung in den Systemen vorzugeben.

In Systemen vorinstallierte Standardpasswörter werden entsprechend dem Dokument "Umgang mit Passwörtern" geändert.

Passwörter werden unverzüglich geändert, sobald sie Unbefugten bekannt geworden sind oder der Verdacht besteht, dass sie Unbefugten bekannt geworden sind. Passwörter sind geheim zu halten. Im Rahmen der Nutzersensibilisierung wird darauf hingewiesen, dass Passwörter nicht mehrfach verwendet werden dürfen, um die Angriffsfläche für Zugänge und Zugriffe zu verringern.

Es wird sichergestellt, dass die mögliche Passwortlänge vom IT-System vollständig geprüft wird. Bei erfolglosen Anmeldeversuchen gibt das System keinen Hinweis darauf, dass das Passwort oder die Benutzerkennung falsch sind.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Schutz von Benutzerkennungen mit weitreichenden Berechtigungen (ORP.4.A10)

Der kompromittierende Zugriff auf Systeme durch Benutzer mit administrativen Rechten ist durch die Verwendung einer dem Stand der Technik entsprechenden Mehrfaktor-Authentisierung zu verhindern.

### Zurücksetzen von Passwörtern (ORP.4.A11)

Für das Zurücksetzen von Passwörtern ist ein angemessenes und sicheres Verfahren zu definieren und zu implementieren. Die Mitarbeitenden der <Institution>, die Passwörter zurücksetzen können, sind in den definierten Prozessen und im Umgang mit den verwendeten Tools zu schulen.

Bei höherem Schutzbedarf des Passwortes ist eine Strategie für den Fall zu definieren, dass der Mitarbeitende aufgrund fehlender sicherer Möglichkeiten zur Übermittlung des Passwortes die Verantwortung nicht übernehmen kann.

### Entwicklung eines Authentisierungskonzeptes für IT-Systeme und Anwendungen (ORP.4.A12)

Das Authentisierungskonzept definiert die funktionalen und sicherheitstechnischen Anforderungen an die Authentisierung für jedes IT-System und jede Anwendung. Die Authentisierungsinformationen werden nur mit den intern freigegebenen Verfahren und Protokollen verschlüsselt übertragen.

### Geeignete Auswahl von Authentisierungsmechanismen (ORP.4.A13)

Die Art der Authentisierung an Systemen und Anwendungen richtet sich nach deren Schutzbedarf. Die Authentisierungsdaten müssen durch das IT-System bzw. die IT-Anwendungen während der Verarbeitung jederzeit vor Ausspähung, Veränderung und Vernichtung geschützt sein.

### Kontrolle der Wirksamkeit der Benutzertrennung am IT-System bzw. Anwendung (ORP.4.A14)

Anhand von Informationen aus IT-Systemen und Anwendungen ist zu prüfen, ob sich Benutzer nach Erledigung ihrer Aufgaben vom System abmelden oder ob sich Benutzer mit derselben Kennung an mehreren Systemen angemeldet haben.

### Vorgehensweise und Konzeption der Prozesse beim Identitäts- und Berechtigungsmanagement (ORP.4.A15)

Für das Identitäts- und Berechtigungsmanagement sind Prozesse zu definieren, die für die Verwaltung von Richtlinien, Identitätsprofilen, Benutzerkennungen, Berechtigungsprofilen und Rollen gelten.

### Richtlinien für die Zugriffs- und Zugangskontrolle (ORP.4.A16)

Im Standard „IT-Administration“ sind die Grundsätze der Zugriffs- und Zugangskontrolle festgelegt.

Für jedes System und jede IT-Anwendung existiert eine schriftliche Zugriffsregelung.

Alle Zugriffsrechte aller Benutzer sind zentral dokumentiert. Der Zugriff auf Systeme und Anwendungen ist nur nach erfolgreicher und angemessener Identifizierung und Authentifizierung möglich.

### Geeignete Auswahl von Identitäts- und Berechtigungsmanagement-Systemen (ORP.4.A17)

Die Auswahl des Berechtigungsmanagementsystems erfolgt unter Berücksichtigung der Geschäftsprozesse, Organisationsstrukturen und Abläufe sowie deren Schutzbedarf.

Das Identitäts- und Berechtigungsmanagementsystem stellt den Prozess der Vergabe von Identitäten und Berechtigungen sicher und unterstützt den Grundsatz der Funktionstrennung und die Anforderungen an die Datensicherheit.

### Einsatz eines zentralen Authentisierungsdienstes (ORP.4.A18)

Als zentrales Identitäts- und Berechtigungsmanagement wird ein zentraler netzbasierter Authentisierungsdienst eingesetzt.

Alle Sicherheitsanforderungen an das System und dessen Auswahlprozess sind dokumentiert.

### Einweisung aller Mitarbeiter in den Umgang mit Authentisierungsverfahren und -mechanismen (ORP.4.A19)

Alle Nutzer sind im Umgang mit den Authentisierungsverfahren geschult und werden über relevante Änderungen informiert.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Notfallvorsorge für das Identitäts- und Berechtigungsmanagement-System (ORP.4.A20)

Für das Identitäts- und Berechtigungsmanagementsystem sind Notfallpläne zu entwickeln, da es für die Sicherheit und Stabilität der Geschäftsprozesse kritisch ist. Wird die eingesetzte Lösung von einem Dienstleister oder mittels SaaS betrieben, sind die Notfallpläne darauf abzustimmen.

Die Notfallpläne sind regelmäßig zu überprüfen und Notfallübungen sind regelmäßig durchzuführen.

### Mehr-Faktor-Authentisierung (ORP.4.A21)

Unter Berücksichtigung des Schutzbedarfs der Zugänge und Zugriffe auf IT-Systeme und Anwendungen und deren Informationen wird für die Anmeldung eine dem Stand der Technik entsprechende Mehr-Faktor-Authentifizierung implementiert.