Zugangsrichtlinie (BASIC)

 Vorlage

# Autorität und Überprüfung

## Dokumentenkontrolle und -prüfung

|  |  |
| --- | --- |
| **Dokumentenprüfung**  |  |
| Autor  |  |
| Eigentümer |  |
| Datum der Erstellung |  |
| Zuletzt überarbeitet von  |  |
| Datum der letzten Überarbeitung |  |

## Versionsverwaltung

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Datum der Genehmigung** | **Genehmigt durch**  | **Beschreibung der Änderung** |
| 1.0 |  |  |  |

# Intro

Innerhalb von **[Organisation]** ist die Zugriffsverwaltung eine wesentliche Komponente der Sicherheit. Sie legt fest wer unter welchen Umständen Zugang zu bestimmten Daten, Anwendungen und anderen digitalen Ressourcen hat. Diese Zugriffsverwaltungsrichtlinien sichern digitale Umgebungen auf dieselbe Weise, wie Schlüssel und Gästelisten physische Räume sichern. Mit anderen Worten: Sie lassen die richtigen Personen hinein und halten andere Personen fern. Diese Richtlinien beruhen auf Techniken wie Authentifizierung und Autorisierung. Damit kann **[Organisation]** überprüfen, ob die Benutzer die sind, für die sie sich ausgeben, und ob diesen Benutzern ein angemessener Zugang gewährt wurde, basierend auf Informationen wie Gerät, Standort, Funktion und mehr.

Dieses Strategiedokument ist Teil einer Reihe von Strategiedokumenten, die **[Organisation]** bei der Entwicklung einer soliden Cybersicherheitsstrategie unterstützen.

# Verwaltung des Zugangs

**[Organisation]** wendet den Grundsatz des minimalen Zugangs an. Das bedeutet, dass jeder interne oder externe Nutzer innerhalb von **[Organisation]** genau den Zugang zu den Informationen und Systemen erhält, den er benötigt, um seine Funktion ordnungsgemäß auszuführen. Darüber hinaus bevorzugt **[Organisation]** dieImplementierung und Einsetzung der standardmäßigen Multi-faktor-Authentifizierung (MFA) überall wo dies möglich ist.

Der Fernzugriff auf kritische und vertrauliche Systeme von **[Organisation]** von einem nicht vertrauenswürdigen Ort aus, z.B. von Zuhause oder aus dem Büro eines Kunden, sollte auf bestimmte Benutzer beschränkt werden. Die Laptops der **[Organisation]** sind mit Einstellungen für den Aufbau einer VPN-Verbindung zu den Systemen der **[Organisation]** ausgestattet.

Die gewährten Zugänge werden in regelmäßigen Abständen überprüft und falls erforderlich geändert. Anpassungen in Bezug auf den Zugang, einschließlich der Fernarbeit, werden der **[in der Organisation verantwortlichen Person]** rechtzeitig mittels eines Formulars zur Einrichtung/Änderung eines Kontos (ACMF) oder eines Formulars zur Entfernung eines Kontos (ARF) mitgeteilt **(siehe ANHANG 1 Formulare**)

# Kontoführung

## Benutzerkonten

Benutzerkonten sind ein gängiges Mittel zur Authentifizierung. Die folgenden Regeln gelten für Benutzerkonten für den Zugriff auf kritische und vertrauliche Systeme:

* Sie sollten einzigartig und persönlich sein.
* Sie müssen passwortgeschützt sein, wie in der Passwortrichtlinie beschrieben.
* Neue Benutzerkonten für Mitarbeiter können nur von einer autorisierten Person beantragt und bearbeitet werden.
* Sie sollten entfernt werden, wenn sie veraltet sind (z. B. bei Beendigung des Vertrags).

## Privilegierte Konten

Die Zuweisung von Konten mit Privilegien (z. B. Domänenadministrator, Superuser und root) sollte eingeschränkt werden. Privilegierte Konten sollten nur verwendet werden, wenn ein privilegierter Zugriff erforderlich ist. Die Inhaber solcher Konten sollten ein nicht privilegiertes Konto für normale Benutzeraktivitäten verwenden. So sollten beispielsweise Systemadministratoren ihr Domänenadministrator-Konto nicht für die Bearbeitung ihrer E-Mails verwenden.

Der Name dieses Kontos sollte keine Informationen über die erweiterten Berechtigungen des Kontos preisgeben, um Missbrauch zu verhindern.

Für privilegierte Konten für kritische und vertrauliche Systeme, auf die von nicht vertrauenswürdigen Netzwerken wie dem Internet aus zugegriffen wird, sollte eine mehrstufige Authentifizierung verwendet werden.

## Gemeinsame Konten

Die Nutzung von Gemeinsamen Konten sollte verhindert werden. Lässt sich dies nicht verhindern, sollte ihre Nutzung kontrolliert werden. Es sollten Kontrollen vorhanden sein, um:

* Zu wissen, wer das Konto nutzen kann.
* Die Nutzung des Kontos zu kontrollieren.
* Einen Prozess der Passwortänderung und Mitteilung des neuen Passworts zu haben.
* Missbrauch, z. B. bei Beendigung des Vertrags zu verhindern.

## Konten für externe Mitarbeiter und externe Unternehmen

Bei Konten für externe Mitarbeiter sollten folgende zusätzliche Kontrollen durchgeführt werden:

* Diese Konten sollten leicht als solche für externe Mitarbeiter erkennbar sein, z. B. durch ein Präfix in der Kontobezeichnung oder durch einen Hinweis in der Beschreibung.

Diese Konten müssen am Ende des Vertrages gekündigt werden. Kann dieser Prozess nicht vollständig gewährleistet werden, sollte das Konto automatisch alle **[3 Monate]** auslaufen, sofern keine offizielle Verlängerung genehmigt wird.

## Dienstkonten für die Kommunikation zwischen Systemen

Die folgenden zusätzlichen Kontrollen sollten für Dienstkonten und Konten für die Maschine-zu-Maschine-Kommunikation vorhanden sein:

* Diese Konten sollten leicht als Dienstleistungskonto zu erkennen sein, z. B. durch Hinzufügen eines Präfixes zum Kontonamen oder durch Erwähnung in einer Beschreibung.
* Auch hier gilt der Grundsatz des Mindestzugangs.
* Die interaktive Nutzung von Dienstkonten sollte vermieden werden.

# Authentifizierung und Autorisierung

**Microsoft Active Directory (AD)** ist eine zentralisierte Authentifizierungs- und Autorisierungslösung, die die Verwaltung von Rechten und Sicherheitseinstellungen in einem Netzwerk ermöglicht. AD ist in die Windows-Umgebung integriert und ermöglicht die delegierte Verwaltung der Windows-Umgebung von **[Organisation].**

## Authentifizierung

* Durch ein sicheres Verbindungsverfahren sollte es möglich sein, den Zugang zu Systemen und Anwendungen zu kontrollieren.
* Der **[IT-Manager]** muss jeden Verbindungsversuch aufzeichnen und überwachen, unabhängig davon, ob er erfolgreich ist oder nicht.
* Ursprüngliche Passwörter sollten sicher und direkt an den Nutzer übermittelt werden.
* Ursprüngliche Passwörter sind so eingestellt, dass sie sofort geändert werden.
* Wo es sinnvoll und machbar ist, sollte eine Multi-faktor-Authentifizierung verwendet werden.
* Das Benutzerkonto sollte für einen vorher festgelegten Zeitraum gesperrt werden, wenn der Benutzer eine vorher festgelegte Anzahl von fehlgeschlagenen Authentifizierungsversuchen **[3 Versuche]** innerhalb eines vorher festgelegten Zeitraums **[5 Minuten]** unternimmt**.**
* Der Zugang zum System sollte gesperrt werden, wenn das Konto über einen bestimmten Zeitraum **[z. B. 90 Tage]** nicht genutzt wurde.

## Autorisierung

* Die Gewährung oder Verweigerung des Zugangs zu den Informationssystemen kann nur rechtzeitig über ein ACMF/ARF-Formular beantragt werden. (siehe ANHANG 1 Formulare)
* Dieser Zugang kann nur von der zuständigen Personalabteilung oder dem N+1 der betreffenden Person beantragt werden.
* Bevor der Zugang gewährt wird, muss **[zuständige Organisation]** formell zustimmen. Der **[IT-Verantwortliche]** muss Zugriffsrechte gewähren, aktualisieren und entziehen.
* Es werden so weit wie möglich Berechtigungsgruppen verwendet, und der Zugang wird auf Grundlage von Rollen gewährt.