# **Zugriffsrichtlinie (Access Control Policy)**

## **1. Ziel der Richtlinie**

Diese Zugriffsrichtlinie definiert die Regeln und Verfahren, um sicherzustellen, dass der Zugriff auf Unternehmensressourcen kontrolliert und geschützt ist. Ziel ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten und das Risiko unbefugter Zugriffe zu minimieren.

## **2. Geltungsbereich**

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Partner und externen Dienstleister, die Zugriff auf die IT-Systeme, Anwendungen, Netzwerke und physischen Einrichtungen des Unternehmens haben.

## **3. Grundprinzipien**

1. **Need-to-Know-Prinzip:** Zugriff wird nur auf Basis der beruflichen Notwendigkeit gewährt.
2. **Least Privilege-Prinzip:** Benutzer erhalten nur die minimalen Berechtigungen, die sie für ihre Aufgaben benötigen.
3. **Kontrollierte Zugriffserteilung:** Jede Zugriffsanfrage wird geprüft und dokumentiert.
4. **Regelmäßige Überprüfung:** Alle Zugriffsberechtigungen werden regelmäßig überprüft und bei Bedarf angepasst.

## **4. Rollen und Verantwortlichkeiten**

1. **IT-Abteilung:**

* Verwaltung und Überwachung von Benutzerkonten und Zugriffsrechten.
* Einrichtung und Deaktivierung von Zugriffen gemäß den Unternehmensrichtlinien.

2. **Abteilungsleiter:**

* Genehmigung von Zugriffsanfragen.
* Sicherstellen, dass Mitarbeiter nur auf die für ihre Arbeit relevanten Ressourcen zugreifen können.

3. **Mitarbeiter:**

* Verantwortungsvoller Umgang mit ihren Zugangsdaten.
* Melden von unbefugtem Zugriff oder verdächtigen Aktivitäten.

4. **Compliance-Team:**

* Überwachung der Einhaltung dieser Richtlinie und Durchführung von Audits.

## **5. Zugriffsarten und Regeln**

**5.1 Benutzerkonten**

* **Mitarbeiterkonten:** Jeder Mitarbeiter erhält ein individuelles Benutzerkonto. Gemeinsame Konten sind verboten.
* **Gastkonten:** Gastkonten werden nur in Ausnahmefällen und mit zeitlicher Begrenzung eingerichtet.
* **Externe Dienstleister:** Externe Benutzer erhalten zeitlich begrenzte Konten mit spezifischen Zugriffsbeschränkungen.

**5.2 Authentifizierung**

• **Passwörter:**

• Mindestlänge: 12 Zeichen.

• Komplexität: Kombination aus Groß-/Kleinbuchstaben, Zahlen und Sonderzeichen.

• Gültigkeitsdauer: 90 Tage.

• **Multi-Faktor-Authentifizierung (MFA):**

• MFA ist für alle Benutzerkonten obligatorisch.

**5.3 Zugriffserteilung**

* Alle Zugriffsanfragen müssen durch den Vorgesetzten genehmigt und von der IT-Abteilung dokumentiert werden.
* Zugriffe werden nach dem Prinzip der minimalen Berechtigungen erteilt.

**5.4 Zugriffskontrolle**

* **Physische Ressourcen:** Zugang zu Serverräumen wird durch elektronische Schlüsselkarten und biometrische Authentifizierung geregelt.
* **IT-Systeme:** Zugriff wird durch Firewalls, Role-Based Access Control (RBAC) und Netzwerksegmentierung kontrolliert.

**5.5 Zugriffsentzug**

* Zugriffsrechte werden bei Beendigung des Arbeitsverhältnisses oder nach Abschluss eines Projekts sofort entzogen.
* Accounts von inaktiven Benutzern werden nach 30 Tagen deaktiviert.

## **6. Überwachung und Auditierung**

1. **Protokollierung:**

* Alle Zugriffsvorgänge werden in SIEM-Systemen protokolliert.
* Anomalien werden durch automatische Alarme hervorgehoben.

2. **Audit:**

* Quartalsweise Überprüfung der Zugriffsliste durch die IT-Abteilung und das Compliance-Team.
* Ergebnisberichte werden an die Geschäftsführung übermittelt.

## **7. Schulung und Awareness**

* Alle Mitarbeiter müssen jährlich an Schulungen zu Zugangssicherheit teilnehmen.
* Neue Mitarbeiter erhalten beim Onboarding eine Einweisung in diese Richtlinie.

## **8. Konsequenzen bei Verstößen**

* Unbefugte Nutzung oder Weitergabe von Zugangsdaten führt zu Disziplinarmaßnahmen, die bis zur Kündigung reichen können.
* Schwere Verstöße können rechtliche Schritte nach sich ziehen.

## **9. Gültigkeit und Überprüfung**

Diese Richtlinie tritt am [Datum] in Kraft und wird jährlich durch das Compliance-Team überprüft. Änderungen müssen von der Geschäftsführung genehmigt werden.

## **10. Genehmigung**

**Name:** [Name des Genehmigenden]

**Position:** [Position]

**Datum:** [Datum]

**Unterschrift:** [Unterschrift]

Dieses Policy-Dokument bietet klare Anweisungen und setzt Standards für den Zugriff auf Unternehmensressourcen, die nicht nur die Sicherheit erhöhen, sondern auch regulatorische Anforderungen erfüllen.