

RICHTLINIE ZUR VERWALTUNG VON BERECHTIGUNGEN UND BENUTZERRECHTEN



RICHTLINIE ZUR VERWALTUNG VON BERECHTIGUNGEN UND BENUTZERRECHTEN

1. ZWECK

Innerhalb des Unternehmens die Rechte der Benutzer und die Regeln für die Erlangung von Berechtigungen festzulegen.

2. ANWENDUNGSBEREICH

Umfasst alle Benutzer und Abteilungen, die die IT-Ressourcen nutzen.

3. VERANTWORTLICHE

Die gesamte Geschäftsleitung ist dafür verantwortlich, dass alle Mitarbeiter in Übereinstimmung mit dieser Richtlinie handeln.

4. ANWENDUNG

4.1. Berechtigungsverwaltung

Berechtigungen sind ausschließlich auf Ordnerzugriff, Softwareinstallation, Verbindungszeiten, Netzwerkeinstellungen, allgemeine Internetnutzung, Gäste-Internetzugang sowie Remote-Arbeit/-Zugriff beschränkt. Sie werden mindestens alle 12 Monate überprüft, und zudem erfolgen bei Eintritt, Austritt oder Aufgabenwechsel eines Mitarbeiters erneute Autorisierungen.

Berechtigungsverwaltung: Für Führungskräfte;

- * Die Anfrage wird an den Manager weitergeleitet. Der Manager sendet dem Systemadministrator ein Genehmigungsschreiben zur Bearbeitung der Anfrage.

Berechtigungsverwaltung: Für Unternehmensmitarbeiter;

- * Der Mitarbeiter stellt den Berechtigungsantrag bei seinem Vorgesetzten.
- * Stimmt der Vorgesetzte zu, wird die Anfrage an den Manager weitergeleitet.
- * Nachdem der Manager die Anfrage geprüft hat, sendet er bei Zustimmung ein Genehmigungsschreiben für die Berechtigung an den IT-Dienstleister.
- * Das Berechtigungszugriffsrecht wird für die vom Manager festgelegte Dauer gewährt. Nach Ablauf dieser Frist wird das gewährte Recht vom IT-Dienstleister entzogen.

Berechtigungsverwaltung: Für Dienstleister;

- * Der zuständige Vorgesetzte des Dienstleisters stellt den Berechtigungsantrag.
- * Die Anfrage wird an den Manager weitergeleitet.
- * Das Berechtigungszugriffsrecht wird für die vom Manager festgelegte Dauer gewährt. Nach Ablauf dieser Frist wird das gewährte Recht vom IT-Dienstleister entzogen.

RICHTLINIE ZUR VERWALTUNG VON BERECHTIGUNGEN UND BENUTZERRECHTEN

1.1. Benutzerrechte

Softwareinstallation

- * Das Speichern oder Installieren von nicht arbeitsbezogener Software (einschließlich Installationsdateien) ist unter allen Umständen untersagt.
- * Benutzer dürfen, auch wenn dies technisch möglich ist, ohne Genehmigung des Managers keine Software auf ihren Computern installieren, da dies zu Urheberrechtsverletzungen und technischen Problemen führen kann.
- * Besteht die Notwendigkeit, Software für berufliche Zwecke zu installieren, müssen die Stellungnahme und Genehmigung des IT-Dienstleisters eingeholt werden.
- * Software wie Sicherheitsanalyse- und Systemverwaltungssoftware wird ausschließlich vom IT-Dienstleister auf Computern und Arbeitsstationen installiert. Die Installation erfolgt mit Genehmigung des Managers.
- * Die Installation und Nutzung von Systemhilfsprogrammen ist ausschließlich der IT-Abteilung gestattet.
- * Systemhilfsprogramme werden ausschließlich zur Behebung von Benutzerproblemen installiert und verwendet. Sie werden nicht für die Systemverwaltung eingesetzt.
- * In sehr speziellen Fällen können bei Bedarf an Remote-Arbeit mit eingeschränkter Zugriffsberechtigung Systemhilfsprogramme verwendet werden. In diesem Fall müssen ein Antrag gestellt und die Genehmigung des Managers eingeholt werden.
- * Nach Abschluss des Vorgangs wird das Systemhilfsprogramm unverzüglich beendet.
- * Die Verbindungszeiten für die Nutzung der Software werden mit den zuständigen Software-Verantwortlichen vereinbart. Sie gelten für die innerhalb der Domäne definierten Gruppen.

Konfigurations- und Sicherheitseinstellungen

- * Benutzer dürfen, auch wenn dies technisch möglich ist, das Sicherheitsniveau der Einstellungen auf ihren Computern nicht herabsetzen.
- * Als Beispiele für Sicherheitseinstellungen;
 - o Sicherheitszoneneinstellungen, die MS Internet Explorer und MS Outlook betreffen (Internet Explorer Securityzone Settings),
 - o Einstellungen des Virenschutzprogramms,
 - o Einstellungen für Betriebssystemaktualisierungen,
 - o Einstellungen der persönlichen Firewall,
 - o BIOS-Einstellungen sowie weitere hardware- und softwarebezogene Sicherheitseinstellungen genannt werden.

RICHTLINIE ZUR VERWALTUNG VON BERECHTIGUNGEN UND BENUTZERRECHTEN

- * Benutzer dürfen, auch wenn dies technisch möglich ist, über ihre persönlichen Computer keine neuen Netzwerkdienste (wie Webserver, Datenbankserver) betreiben.
- * Sie dürfen auf ihren Computern keine neuen Benutzer und Benutzergruppen anlegen und die Rechte bestehender Benutzer und Benutzergruppen nicht ändern.
- * Ist aufgrund ihrer Bedürfnisse eine Änderung der Konfigurations- und Sicherheitseinstellungen erforderlich, müssen zwingend die Stellungnahme und Genehmigung des IT-Dienstleisters eingeholt werden.
- * Änderungen an Konfigurations- und Sicherheitseinstellungen dürfen nur durch den IT-Dienstleister und nur für die erforderliche Dauer vorgenommen werden.

Recht auf Zugang zu Netzwerken und Netzwerkdiensten

- * Die Zugriffsrechte der Benutzer in unserem Unternehmen sind auf den Bereich ihrer eigenen Abteilung beschränkt.
- * Zugriffsbeschränkungen werden über Active Directory verwaltet.
- * Es wurden Berechtigungstabellen für die Zugriffsbeschränkungen erstellt, deren Kontinuität sichergestellt wird und die nach beschäftigungsbezogenen Änderungen überprüft werden.
- * Der Zugriff auf Drucker und ähnliche Ressourcen über das Netzwerk wird vom IT-Dienstleister konfiguriert.
- * Wird über das Netzwerk der Zugriff auf Anwendungen in anderen Subnetzen benötigt, wird dieser Zugriff vom IT-Dienstleister konfiguriert.
- * Lokale Administratorrechte wurden mit Ausnahme der Gruppe „Poweruser/Local Admin“ entfernt.
- * Die Zugehörigkeit zur Gruppe der Poweruser gilt für die vom Manager festgelegte Dauer.
- * Für das Recht auf Zugehörigkeit zur Gruppe der Poweruser stellt der Benutzer zunächst einen Antrag bei seinem administrativen Vorgesetzten. Hält der administrative Vorgesetzte den Antrag für angemessen, spricht er mit dem Manager.
- * Hält der Manager den Antrag für angemessen, eröffnet er über den Helpdesk einen Vorgang beim IT-Dienstleister.

Dokumentzugriffsrecht

Auf Grundlage der von der Personalabteilung übermittelten Mitteilung über einen Aufgabenwechsel müssen die Zugriffseinstellungen für den bisherigen Abteilungsordner entfernt und die Zugriffseinstellungen für den neuen Abteilungsordner vorgenommen werden.

RICHTLINIE ZUR VERWALTUNG VON BERECHTIGUNGEN UND BENUTZERRECHTEN

Handelt es sich um einen neuen Mitarbeiter, muss von der Personalabteilung eine schriftliche Anfrage (per E-Mail) darüber eingeholt werden, für welchen Ordner und welche Ordnerberechtigungen Zugriff gewährt werden soll. Ohne schriftliche Anfrage wird keine Änderung der Zugriffsrechte vorgenommen.

Der IT-Dienstleister ist verpflichtet, die Dokumentzugriffsrechte aller Computerbenutzer mindestens einmal alle 12 Monate sowie bei Aufgabenwechseln zu überprüfen und zu autorisieren.

4.3. Ordnerzugriffsrechte

- * Es wurde so konfiguriert, dass nur Benutzer, die Teil der Domäneninfrastruktur sind, Zugang zu den Ordnern erhalten.
- * Für die für jede Abteilung eingerichteten Ordner haben die Benutzer der jeweiligen Abteilung volle Berechtigung, während der Zugriff auf Ordner anderer Abteilungen von der Genehmigung des Managers abhängt.

Gerätenutzung

- * Im Rahmen der Benutzerrechte sind die USB-Anschlüsse (externe Datenträger) aller Benutzer deaktiviert. Bei Bedarf werden mit Genehmigung des zuständigen Managers durch den IT-Dienstleister befristete und zahlenmäßig begrenzte Berechtigungen erteilt.
- * Ist die Nutzung zwingend erforderlich, wird das Nutzungsrecht gemäß der Berechtigungsverwaltung gewährt. Die Verantwortung liegt beim Benutzer.
- * Berater, Kunden und Besucher werden nicht in das Unternehmensnetzwerk aufgenommen.
- * Die Nutzung von Geräten durch Dienstleister unterliegt einer Genehmigung, wobei die Berechtigungsverwaltung angewendet wird.
- * Über die Domäne ist eine „Geräteerkennungsrichtlinie“ aktiv. Für jedes verbundene Gerät wird ein Protokoll geführt.