B to B - Praxistools für Unternehmen und Freiberufler

knowNOW
TOOLS FOR BUSINESS SUCCESS

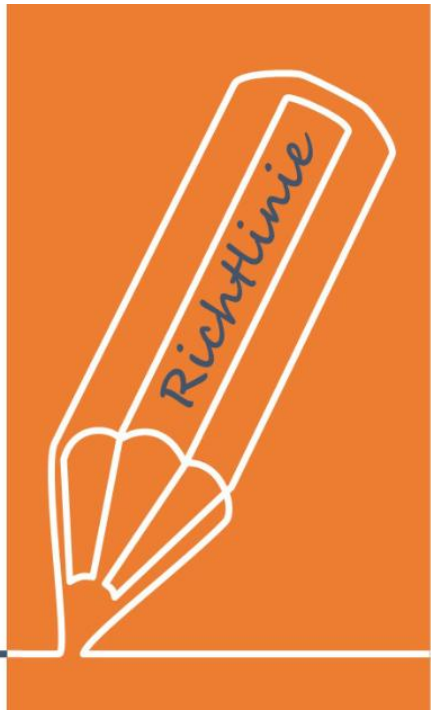
Richtlinie Bereitstellung von Benutzerzugängen

UseNOW - TeachNOW - LearnNOW - FindNOW

- Sofort nutzbar: Auswählen - Anpassen - Anwenden
- In der Praxis erprobt und bewährt
- Im Tagesgeschäft sofort anwendbare Hilfsmittel
- Aktuell durch regelmäßige Updates

Richtlinie Bereitstellung von Benutzerzugängen

des Unternehmens



Inhaltsverzeichnis

- **Führungskräfte / Prozessverantwortliche:**
  Verantwortlich für die Genehmigung von Zugriffsanfragen und die regelmäßige Überprüfung von Zugriffsrechten.

- **Informationssicherheitsbeauftragte(r):**
  Verantwortlich für die Beratung der Führungskräfte / Prozessverantwortlichen im Zusammenhang mit der Vergabe von Zugriffsrechten.

- **IT-Abteilung, IT-Dienstleister:**
  Verantwortlich für die Einrichtung und Verwaltung von Benutzerkonten und Zugriffsrechten.

- **Beschäftigte:**
  Verantwortlich für den sicheren Umgang mit ihren Anmeldeinformationen und die Meldung von Sicherheitsvorfällen bzw. Verdachtsfällen.

4. Zugriffserteilung bzw. Benutzerkonten

Neue Benutzerkonten müssen von der jeweiligen Führungskraft oder der obersten Leitung schriftlich genehmigt werden. Berechtigungen sollten nach dem Prinzip der geringsten Rechte (Least Privilege) gewährt werden:

- Beschäftigte erhalten nur die minimalen Rechte, die sie für ihre Arbeit benötigen. Dies verringert das Risiko von Missbrauch oder versehentlich erzeugtem Schaden.
- Zur Vereinfachung der Rollenverwaltung sollte (Role Based Access Control (RBAC) sollten vordefinierte Rollen mit spezifischen Berechtigungen festgelegt werden. Diese lassen sich leichter verwalten und Benutzerkonten somit effizienter organisieren.

Falls Beschäftigte ihre Rolle oder ihren Arbeitsbereich im Falle von Änderungen bzw. Übertragungen in der Organisation wechseln, sollten deren Berechtigungen entsprechend aktualisiert und nicht mehr benötigte Rechte entzogen werden.
Falls Beschäftigte das Unternehmen verlassen oder kein Zugriff mehr benötigt wird, sind die Konten kurzfristig zu deaktivieren und nach einer definierten Frist zu löschen (*siehe auch Richtlinie Beendigung*).

5. Zugangsarten und Passwortverwaltung

Die Festlegung unterschiedlicher Zugangsarten trägt der Organisation die Sicherheit, Effizienz und Compliance zu gewährleisten. Sensible Daten und Systeme können durch Isolierung kritischer Systeme nur für berechtigte Benutzer / Benutzerinnen zugänglich gemacht werden. So wird der potentielle Schaden durch Insider-Beziehungen oder kompromittierte Konten reduziert. Standardbenutzer / Standardbenutzerinnen ohne administrative Rechte können durch unbeabsichtigte menschliche Fehler keine kritischen Änderungen an Systemen vornehmen, oder Daten weitergeben. Somit wird nicht zuletzt die Einhaltung von Datenschutzbestimmungen gewährleistet.

Die folgenden Zugänge sind zu unterscheiden:

- **Standardbenutzer / Standardbenutzerinnen:**
  Zugriff auf Standardressourcen, die für die tägliche Arbeit benötigt werden.
- **Administrativer Zugriff:**
  Nur für IT-Mitarbeiter und bestimmte Führungskräfte, die spezielle Aufgaben erfüllen müssen.
- **Gastzugänge:**
  Temporäre Zugänge für externe Berater oder Partner, zeitlich und thematisch begrenzt und überwacht. Im Idealfall sollten diese Konten nach einem festgelegten Zeitraum automatisch deaktiviert werden.

Durch Festlegung dieser Zugangsarten ist es einfacher, bestimmte Gruppen von Benutzern / Benutzerinnen mit vorab definierten Berechtigungen zu versehen, anstatt für jeden Benutzer / Benutzerin individuell Zugriffe zu konfigurieren.

Bei der Erstellung eines neuen Kontos sollten Benutzer / Benutzerinnen dazu gezwungen werden, ein starkes Passwort zu wählen, das den Unternehmensrichtlinien entspricht.

Detaillierte Vorgaben hierfür sind in der „Richtlinie zur Nutzung von Kennwörtern“ dokumentiert.

6. Verwaltung von privilegierten Konten

Für privilegierte Konten mit Zugang zu sensiblen Systemen sollten strengere Sicherheitsmaßnahmen wie Mehrfaktor-Authentifizierung (MFA) und spezielle Monitoring-Systeme eingerichtet werden.
Administratoren und andere Benutzer / Benutzerinnen mit erweiterten Rechten sollten separate Konten für administrative und reguläre Aufgaben verwenden.

7. Zugriffskontrolle

Es erfolgt eine regelmäßige Überprüfung und Aktualisierung der Benutzerrechte.

Alle Aktionen, die auf Benutzerkonten ausgeführt werden (Erstellung, Änderungen, Anmeldeversuche, Zugriffe auf sensible Daten), sollten detailliert protokolliert werden. Diese Protokolle sollten regelmäßig analysiert werden, um verdächtige Aktivitäten oder Sicherheitsverstöße frühzeitig zu erkennen.

8. Sperrung von Benutzerkonten und Deaktivierungen

Alle Beschäftigten sind verpflichtet, Sicherheitsverletzungen oder verdächtige Aktivitäten sofort zu melden. Bei Verdacht auf Missbrauch oder Sicherheitsverletzungen ist die sofortige Sperrung von betroffenen Konten zu prüfen.

- Konten sollten automatisch gesperrt werden, wenn mehrere fehlgeschlagene Anmeldeversuche auftreten, um Brute-Force-Angriffe zu verhindern.

Benutzerkonten, die über einen festgelegten Zeitraum von 90 Tagen nicht verwendet wurden, sollten überprüft und im Zweifel deaktiviert werden (*siehe auch Richtlinie Clean-Desk*). Es sind sichere Prozesse zu implementieren, um ein gesperrtes Konto wiederherzustellen oder einem Benutzer nach einem verlorenen Passwort wieder Zugang zu gewähren.

9. Überprüfung, Sensibilisierung und Verbesserung

Diese Richtlinie wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen Bedrohungen und gesetzlichen Anforderungen entspricht. Im Rahmen der Schulungsplanung finden regelmäßige Schulungen und Sensibilisierungsprogramme für alle Beschäftigten statt, um das Bewusstsein für die beste Praxis bei der Verwaltung von Benutzerkonten zu fördern.

Nichteinhaltung dieser Richtlinie kann zu disziplinarischen Maßnahmen führen, einschließlich Abmahnung, Kündigung oder rechtlichen Schritten.

10. Dokumentenlenkung und Änderungshistorie

Diese Richtlinie wird durch das Informationssicherheitsteam gelenkt.

Dokumentenlenkung

Klassifizierung der Vertraulichkeit (1-10)	
Klassifizierung der Vertraulichkeit	☐ Öffentlich ☐ Intern ☐ Vertraulich ☐ Streng vertraulich
Speicherort	[z.B. URL der Datei auf dem Server]
Verantwortlicher	
Aktuelle Version	1.0
Datum Erstellung / letzte Änderung	19.11.2025
Nächstes Dokumenten-Review	19.11.2026

Dokumentenhistorie

Version	Freigegeben am	Freigegeben durch	Kommentar
1.0	19.11.2025		

Hinweise zur Nutzung der Vorlage

Diese Arbeitshilfe soll nur eine ausführliche Vorlage für eine „Richtlinie Bereitstellung von Benutzerzugängen“ darstellen. Sie wurde nach bestem Wissen und Gewissen recherchiert, zusammengestellt und überprüft. Sie erhebt aber keinen Anspruch auf Vollständigkeit oder Eignung für den Einzelfall und erlaubt keine ausschließliche Anwendbarkeit für ein Unternehmen.

Jede Person, die dieses Produkt erwirbt ist verpflichtet, ihre individuellen Ergänzungen und Anpassungen vorzunehmen und alle Inhalte für den eigenen Anwendungsfall zu prüfen, d.h. diese ggf. mit eigenen Texten zu erweitern oder nicht passende Inhalte zu entfernen.

Die nachfolgende Liste gibt Ihnen einige Hinweise, worauf Sie bei der Ergänzung mit eigenen Texten bzw. Textmodulen unbedingt achten sollten:

1. Wählen Sie einfache, allgemein verständliche Formulierungen und schreiben Sie keine „Bandwurmsätze“.
2. Benutzen Sie eine verständliche Wortwahl und erklären Sie nicht vermeidbares Fachvokabular.
3. Formulieren Sie nicht zu sehr ins Detail gehend.
4. Geben Sie den Mitarbeitern im Rahmen von Workshops die Gelegenheit auf die Formulierungen Einfluss zu nehmen.
5. Schreiben Sie gendergerecht. Die Nennung aller Geschlechter drückt die Wertschätzung gegenüber allen Menschen aus, unabhängig ihres Geschlechts.

Hinweise zur Anpassung des Dokumentes an die Organisation:

Um das Tool an Ihre Dokumentenstruktur anzupassen, gehen Sie (hier am Beispiel der Version MS Office 2010 dargestellt) bitte folgendermaßen vor:

1. Aktivieren Sie in der Leiste „Start“, Gruppe „Absatz“ das Symbol „Alle anzeigen“. Alternativ können Sie in der Leiste „Datei“ auf „Optionen“ klicken, im sich öffnenden Fenster „Anzeige“ auswählen und das Häkchen bei „alle Formatierungszeichen anzeigen“ setzen.
2. Löschen Sie nun zuerst das Textfeld mit dem Titel und danach die Grafik, indem Sie diese Objekte jeweils markieren und die Entfernen-Taste (Entf) betätigen.
3. Danach löschen Sie den verbliebenen Abschnittswechsel (oben), indem Sie diesen markieren und ebenfalls die Entfernen-Taste (Entf) betätigen.
4. Mittels „Doppelklick“ auf die Kopf- oder Fußzeile können Sie diese nun öffnen und die Texte und deren Formatierungen entsprechend Ihren Wünschen gestalten.
5. Löschen Sie das Kopfzeilen-Logo wie vorher, indem Sie dieses markieren und die Entfernen-Taste (Entf) betätigen.
6. Ein neues Logo fügen Sie ein, indem Sie in der Leiste „Einfügen“, Gruppe „Illustrationen“ auf das Icon „Grafik“ klicken und Ihre Datei auswählen.
7. Diese Hinweisseite entfernen Sie, indem Sie (ab dem letzten Seitenumbruch) alles markieren und die Entfernen-Taste (Entf) betätigen.

Nutzungsbedingungen von Fachinformationen:

(1) Für vorsätzliche oder grob fahrlässige Pflichtverletzungen haftet der Lizenzgeber. Dies gilt auch für Erfüllungsgehilfen.
(2) Für Garantien haftet der Lizenzgeber unbeschränkt.
(3) Für leichte Fahrlässigkeit haftet der Lizenzgeber begrenzt auf den vertragstypischen, vorhersehbaren Schaden.
(4) Der Lizenzgeber haftet nicht für Schäden, mit deren Entstehen im Rahmen des Lizenzvertrags nicht gerechnet werden musste.
(5) Für Datenverlust haftet der Lizenzgeber nur, soweit dieser auch bei der Sorgfaltspflicht entsprechender Datensicherung entstanden wäre.
(6) Eine Haftung für entgangenen Gewinn, für Schäden aus Ansprüchen Dritter gegen den Lizenznehmer sowie für sonstige Folgeschäden ist ausgeschlossen.
(7) Der Lizenzgeber haftet nicht für den wirtschaftlichen Erfolg des Einsatzes der Tools oder Trainings.
(8) Die Haftung nach dem Produkthaftungsgesetz bleibt unberührt.