Berechtigungsverfahren

OA1010

group24 AG (group24)

INHALTSVERZEICHNIS

1 Einleitung 4
1.1 Ziel und Zweck 4
2 Grundsätze der Berechtigungsvergabe 5
2.1 Funktionstrennung 5
2.2 4-Augenprinzip 5
2.3 Need-to-know-Prinzip 5
2.4 Least-Privilege-Prinzip 6
3 Aufgaben und Verantwortlichkeiten 7
3.1 Aufgaben der disziplinarischen Vorgesetzten 7
3.2 Aufgaben der Mitarbeiter 7
3.3 Aufgaben des Bereiches Personal 7
3.4 Aufgaben des Informationssicherheitsbeauftragter (ISB) 8
4 Aufgaben im Mitarbeiter Lifecycle 9
4.1 Eintritt eines Mitarbeiters 9
4.2 Austritt eines Mitarbeiters 9
4.3 Versetzung eines Mitarbeiters innerhalb der group24 9
4.4 Längere Abwesenheit eines Mitarbeiters 10
4.5 Sofortiger Austritt eines Mitarbeiters 10
5 Berechtigungen in den IT-Systemen 11
5.1 User Accounts 12
5.2 User Accounts für externe Mitarbeiter 12
5.2.1 Bereitstellung von Informationen durch den Fachbereich 12
5.2.2 Einrichtung 12
5.3 Administrative Kennungen 12
5.4 Umfang der Jahresprüfung 13
6 Verstösse und Sanktionen 14

STAMMDATEN

Referenz-Nummer:	OA1010
Dokumententitel:	Berechtigungsverfahren
Fachlich Verantwortlicher:	Jens Niehues
Zuständiger Bereich:	Technical Department
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues / Marc Eismann
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung
0.1	01.09.	Sandra Kiemes (extern)	Initiale Erstellung
0.2	16.09.	Andreas Heit	Anpassung auf group24
0.3	28.09.	Andreas Heit	Review mit Fachabteilung
0.4	24.10.	Andreas Heit	Review IT-Security

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues / Marc Eismann	Ersterstellung und Freigabe
V1.1	15.11.2023	Christian Hornhues	Review 2023

1 EINLEITUNG

1.1 Ziel und Zweck

Diese Organisationsanweisung regelt die Vergabe von Berechtigungen von Nicht-administrativen Kennungen innerhalb der group24. Bei der Vergabe von Berechtigungen, die für einen Benutzer an den Arbeitsplätzen der group24 zur Verfügung stehen müssen, folgende Vorgaben beachten werden:

- Anforderungen der „Grundsätze ordnungsmäßiger DV-gestützter Buchführungssysteme" (GoBS),
- das Bundesdatenschutzgesetz (BDSG)

Berechtigungen werden vergeben unabhängig vom Speicherort der Daten für:

- Zugriffe auf Daten der group24 vom Arbeitsplatz aus
- Zugriffe auf Daten der group24 über Administrations-Rechte

2 GRUNDSÄTZE DER BERECHTIGUNGSVERGABE

2.1 Funktionstrennung

Ziel des Prinzips der Funktionstrennung ist der Schutz vor finanziellen Schäden sowie die Einhaltung von regulatorischen Anforderungen. Oberstes Ziel ist die Verhinderung direkten oder indirekten finanziellen Schadens, welcher durch Betrug, Datenmanipulation, Bilanzfälschung, Scheingeschäfte oder auch durch Fehler ohne betrügerischen Hintergrund entstehen kann.

Potenzielle Konflikte sollen erkannt werden und dadurch Risiken eliminiert bzw. verhindert werden. Gewisse Kombinationen von Berechtigungen können einem Benutzer ermöglichen, Aufgaben auszuführen, die – wenn von derselben Person oder organisatorischen Einheit ausgeführt – zu diesen Risiken führen können.

Die Mitarbeiter dürfen nur in den laut Organigramm vorgesehenen Gruppen vertreten sein.

Mitarbeiter der kontrollierenden Einheiten dürfen keine operativen Tätigkeiten im Betrieb durchführen wie z.B. Informationssicherheitsbeauftragter oder auch Datenschutzbeauftragter.

2.2 4-Augenprinzip

Das Vier-Augen-Prinzip, auch Vier-Augen-Kontrolle (englisch Two-man rule) genannt, ist eine Sonderform des Mehr-Augen-Prinzips und besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen werden oder kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen. Ziel ist es, das Risiko von Fehlern und Missbrauch zu reduzieren.

Das Mehr-Augen-Prinzip ist als Prinzip in verschiedenen Bereichen z. B. zur Kontrolle oder Absicherung von Entscheidungen und Tätigkeiten einsetzbar. Es sagt aus, dass entweder eine mehrfache Kontrolle durchgeführt wird oder allgemein mehrere (unabhängige, unvoreingenommene) Personen an der Absicherung einer Entscheidung oder Tätigkeit beteiligt sind. Bei der Umsetzung des Mehr-Augen-Prinzips sind grundsätzlich mehrere Faktoren zu berücksichtigen:

- Unabhängigkeit der Personen
- Unvoreingenommenheit gegenüber dem Prüfgegenstand

2.3 Need-to-know-Prinzip

Das Need-to-know-Prinzip (Kenntnis nur bei Bedarf) beschreibt ein Sicherheitsziel für geheime Informationen. Auch wenn eine Person grundsätzlich Zugriff auf Daten oder Informationen dieser Sicherheitsebene hat, verbietet das Need-to-know-Prinzip den Zugriff, wenn die

Informationen nicht unmittelbar für die Erfüllung einer konkreten Aufgabe von dieser Person benötigt werden.

2.4 Least-Privilege-Prinzip

Das Least-Privilege-Prinzip (oder auch Prinzip der minimalen Privilegien) beschreibt, dass ein Zugriff immer nur mit den geringstmöglichen und nötigen Rechten gewährt wird.

Bsp. Wenn jemand für die Ausübung seiner Tätigkeit keine Schreibrechte benötigt, bekommt er diese auch nicht.

3 AUFGABEN UND VERANTWORTLICHKEITEN

3.1 Aufgaben der disziplinarischen Vorgesetzten

Die disziplinarischen Vorgesetzten in den Geschäftsbereichen haben verantwortlich sicherzustellen, dass die jeweiligen Mitarbeiter lediglich die zur Erfüllung der festgelegten Aufgaben erforderlichen Zugriffsberechtigungen erhalten und dass bei der Anforderung von Benutzerprofilen/-rollen den Erfordernissen der Funktionstrennung (Kapitel 2.1) und/oder des 4-Augen-Prinzips (Kapitel 2.2) Rechnung getragen wird. Die Vergabe der Zugriffsrechte orientiert sich am Need-to-Know-Prinzip (Kapitel 2.3) sowie am 2.4 Least-Privilege-Prinzip (Kapitel 2.4). Dies bedeutet, dass ein Mitarbeiter nur das sehen oder machen darf, was für seine Tätigkeit unmittelbar erforderlich ist.

Bei Ausscheiden eines Mitarbeiters oder bei Versetzungen haben die disziplinarischen Vorgesetzten sicherzustellen, dass Rechte, die nicht über die group24 gelöscht werden können, z.B. Rechte auf externen Plattformen / externen Handelsplattformen, deaktiviert/gelöscht werden.

Bei Versetzungen sind außer den Berechtigungen, die jeder Mitarbeiter hat, sämtliche Benutzerberechtigungen in den IT-Systemen von der neuen Führungskraft zu beantragen.

3.2 Aufgaben der Mitarbeiter

Berechtigungsanforderungen / Löschungen können per Mail an den Service Desk beantragt werden.

3.3 Aufgaben des Bereiches Personal

Der Bereich Personal meldet Personalveränderungen (Personalveränderungsmitteilung) an die Interne IT:

- Eintritt eines neuen Mitarbeiters
- Austritt eines Mitarbeiters
- Versetzung eines Mitarbeiters zu einer anderen oder innerhalb einer Organisationseinheit
    - Hospitanz (befristet) eines Mitarbeiters in einer anderen Organisationseinheit
- längere Abwesenheiten vom Arbeitsplatz
- sofortiger Austritt eines Mitarbeiters
- Namensänderung

Der Bereich Personal informiert bei einer Kündigung den disziplinarischen Vorgesetzten des Mitarbeiters über dessen Kündigung.

3.4 Aufgaben des Informationssicherheitsbeauftragter (ISB)

Wenn innerhalb der Berechtigungsverfahren Ausnahmen genehmigt werden müssen, wird dies durch den Informationssicherheitsbeauftragten geprüft. Dieser prüft die angeforderten Berechtigungen auf Notwendigkeit aus der Funktionsbeschreibung des Mitarbeiters und stellt die Funktionstrennung sicher.

4 AUFGABEN IM MITARBEITER LIFECYCLE

Die nachfolgend beschriebenen Aufgaben beziehen sich nur auf die Mitarbeiter der group24. Der grundlegende Prozess der Personalverwaltung für Ein- und Austritt von Beschäftigten ist im Prozess P3002 Personalprozesse abgebildet.

Nachfolgend werden definierte Berechtigungen und Rollen beschrieben. Alle darüber hinaus gehenden Berechtigungen werden separat betrachtet und beauftragt.

4.1 Eintritt eines Mitarbeiters

Der Auslöser ist eine Personalveränderungsmitteilung an den definierten Verteiler. Die Interne IT richtet folgende Berechtigungen ein:

- Windows-Berechtigungen (Azure) sowie die Berechtigung für Microsoft 365 Office-Produkte (Teams, Word, Excel, Outlook, Powerpoint) und notwendige Einträge für Team-Org-Gruppen, Teamverteiler
- Soweit für die Einheit vorhanden, Zuweisung eines Standardprofils

Bei Wiedereintritt eines Mitarbeiters ist zusätzlich zu prüfen, ob noch „Alt-Berechtigungen /-Profile“ des Mitarbeiters vorhanden sind und ggf. zu löschen.

4.2 Austritt eines Mitarbeiters

Der Auslöser ist eine Personalveränderungsmitteilung an den definierten Verteiler. Die Interne IT löscht folgende Berechtigungen:

- Deaktivierung des Windows-Accounts zum tt.mm.jj
- Löschung aller Berechtigungsprofile zum tt.mm.jj in Systemen, die von group24 verwaltet werden
- Löschung aus den Team-ORGA-Gruppen und Teamverteiler
- Für den Mitarbeiter wird die E-Mail-Adresse deaktiviert
- Der AD-Account, das Mailkonto sowie auch das persönliche Onedrive des Mitarbeiters wird nach 30 Tagen nach Deaktivierung automatisch gelöscht.

4.3 Versetzung eines Mitarbeiters innerhalb der group24

Der Auslöser ist eine Personalveränderungsmitteilung an den definierten Verteiler. Die Interne IT löscht folgende Berechtigungen:

- Löschung aller Berechtigungsprofile zum tt.mm.jj
- Anpassung der Team-Org-Gruppen und des Teamverteilers – es sei denn, der Anwender beantragt die Beibehaltung dieser explizit.
- Löschung von Berechtigungen außerhalb der zentralen Dienste

4.4 Längere Abwesenheit eines Mitarbeiters

Der Auslöser ist eine Personalveränderungsmitteilung an den definierten Verteiler. Die interne IT löscht folgende Berechtigungen:

- Berechtigungsprofile bleiben bei Abwesenheiten von maximal 3 Monaten bestehen
- Abgrenzung des Benutzers Kenjo
- Deaktivierung des Windows-Accounts

4.5 Sofortiger Austritt eines Mitarbeiters

Der Auslöser ist eine Personalveränderungsmitteilung an den definierten Verteiler oder eine sofortige Freistellung.

Interne IT löscht folgende Berechtigungen:

- Deaktivierung des Windows-Accounts (sofort)
- Löschung aller Berechtigungsprofile (sofort)
- Prüfung vorhandener Anmeldungen und erzwungene Abmeldung (sofort)
- Für den Mitarbeiter wird die E-Mail-Adresse deaktiviert
- Erst nach Freigabe durch den Bereich Personal werden AD-Account, Mailkonto und persönliches Onedrive gelöscht.

5 BERECHTIGUNGEN IN DEN IT-SYSTEMEN

Die Umsetzung in den jeweiligen Systemen obliegt den aufgezeigten Einheiten und werden durch die Lifecycle Prozesse des Mitarbeiters ausgelöst. Basis für die beantragten Berechtigungen sind die Anforderungen des Vorgesetzten.

Die Vorgesetzten haben verantwortlich sicherzustellen, dass die jeweiligen Mitarbeiter lediglich die für die Erfüllung der festgelegten Aufgaben erforderlichen Berechtigungen erhalten.

Bezeichnung	Name und Beschreibung	Umsetzende Stelle
Kenjo	Personalverwaltung, Cloudbasierend	Personal
DATEV – Arbeitgeber Online	Gehaltsabrechnung für die Mitarbeiter	Personal
Weclapp	ERP-Plattform, Cloudbasierend	Business Consulting
Telefonanlage 3cx	Telefonanlage (Backend-Komponente)	Interne IT
Azure	Zentrale Gruppen; Berechtigung für Microsoft 365 Office-Produkte, Sharepoint und notwendige Einträge für Team-Org-Gruppen, Teamverteiler	Interne IT
Office 365	Outlook Programme	Interne IT
Last Pass	Passwortverwaltungstool	Interne IT
Logmytime	Zeiterfassung (nur Mitarbeiter Managed Service und Consulting)	Consulting
Menue-Lounge	Bestellung von Mittagsgerichten am Standort Gescher (nur Mitarbeiter Gescher)	Facility Management
Raumzuweisung DOM	Zutrittssteuerung	Facility Management

5.1 User Accounts

Alle User Accounts der group24 werden im Azure Active Directory erstellt und automatisch nach Office 365 synchronisiert.

5.2 User Accounts für externe Mitarbeiter

5.2.1 Bereitstellung von Informationen durch den Fachbereich

Vor der Erstellung der User Accounts für externe Mitarbeiter durch die interne IT, müssen durch den anfordernden Fachbereich folgende Informationen bereitgestellt werden:

- Vorname
- Nachname
- Fachbereich
- Fachlicher Vorgesetzter der group24
- Geplanter Einsatzzeitraum (bis max. 31.12. des laufenden Jahres, Verlängerung möglich)
- O365 Services. Email und Teams werden standardmäßig zugebucht, weitere Services müssen durch die Vorgesetzten) genehmigt werden.

Im Rahmen der Jahresprüfung wird die Rezertifizierung der externen Accounts gemeinsam mit der Fachabteilung ausgeführt.

Erfolgt keine Rückmeldung durch den Fachbereich, werden die entsprechenden User Accounts der externen Mitarbeiter deaktiviert.

Useraccounts für externe Mitarbeiter müssen schriftlich (per Mail) verlängert werden, wenn der Einsatz des externen Mitarbeiters über das Gültigkeitsdatum hinaus notwendig ist. Bei der Verlängerung ist ein neues Gültigkeitsdatum vorzugeben, ein Vertrag muss unterschrieben vorliegen. Bei der Änderung der Kostenstelle muss diese neue angegeben werden.

5.2.2 Einrichtung

Die Einrichtung der O365 Services für externe Mitarbeiter wird erst durchgeführt, wenn vom Externen Mitarbeiter die „Verschwiegenheits-/Einwilligungs-Erklärung“ unterschrieben vorliegt.

Bei einer Verlängerung bleiben die Anwendungsprofile bestehen.

5.3 Administrative Kennungen

In bestimmten Fällen kann es notwendig sein, administrative Berechtigungen zu vergeben. Neben restriktiver Handhabung muss sichergestellt werden, dass eine entsprechende Berechtigung keine negativen Auswirkungen auf die group24 hat.

Administrative Kennungen sind einer jährlichen Prüfung zu unterziehen.

5.4 Umfang der Jahresprüfung

Die Jahresprüfung (Rezertifizierung) umfasst die internen Kennungen sowie die externen Kennungen der Mitarbeiter, die Support im Namen der group24 erbringen. Basis ist das aktuelle Organigramm und die Aufstellung der externen Mitarbeiter.

Die zu prüfenden Berechtigungen sind wie folgt definiert:

- Liste der administrativen Kennungen
- Liste der externen Kennungen
- Liste der Berechtigungen innerhalb der File Services (Teams) der group24
- Liste der Accounts der unter Kapitel 5 definierten IT-Systeme

6 VERSTÖSSE UND SANKTIONEN

Verstöße gegen diese Sicherheitslinie und die darunter liegenden Sicherheitsgrundsätze sind nicht tolerierbar. Sie können daher zu Disziplinarmaßnahmen, arbeitsrechtlichen Maßnahmen oder gar zu Straf- und/oder zivilrechtlichen Verfahren führen.