Afbeelding met tekening

Automatisch gegenereerde beschrijving

**In- en uitdienst**

beleid

|  |  |
| --- | --- |
|  | **Disclaimer**  Dit document kan gebruikt worden als template voor het opzetten van een in- en uitdienst beleid binnen je organisatie. De inhoud van dit document bevat een aantal uitgangspunten die je zou kunnen opnemen in je eigen proces van nieuwe medewerkers, medewerkers die uit dienst gaan en/of medewerkers die van functie wisselen binnen de organisatie. Niet alle uitgangspunten zullen van toepassing zijn, maak daarom een eigen overweging om bepaalde uitgangspunten wel of niet op te nemen in jouw beleid. Naast de input uit dit document is het belangrijk input te verzamelen van de verschillende afdelingen binnen je organisatie (zoals bijvoorbeeld de rol van HR).  **Risico’s**  Wanneer je geen energie steekt in het op orde hebben van het proces van nieuwe medewerkers, medewerkers die uit dienst gaan en medewerkers die binnen jouw organisaties wisselen van functie, loop je het risico dat daar bewust of onbewust incidenten ontstaan. Denk bijvoorbeeld aan de volgende scenario’s:   1. Onbevoegden hebben inzicht in (vertrouwelijke) persoonsgegevens waar je mogelijk ook vanwege wetgeving, zoals de AVG, verplicht bent zorgvuldig mee om te gaan. 2. Naast het inzien van gegevens kunnen medewerkers bestanden waar ze onnodig bij kunnen bewust of onbewust aanpassingen doen of gegevens verwijderen. 3. Medewerkers die uit dienst gaan kunnen na uit dienst datum rechten of toegang tot applicaties en systemen hebben. 4. Beperkt inzicht in de rechten binnen je organisatie kunnen problemen geven wanneer een medewerker uit dienst gaat. Je hebt ook geen overzicht waar iemand toegang toe heeft. 5. Geen goed inzicht in de rechten van medewerkers vergroot de kans op fraude of oneerlijke concurrentie doordat iemand rechten die hij of zij heeft te veel rollen op zich kan nemen.   **Hulpmiddelen**  Als het gaat om nieuwe medewerkers, medewerkers die uit dienst gaan en medewerkers die binnen jouw organisaties wisselen van functie, maak dan bijvoorbeeld gebruik van een ‘rechtenmatrix’. Dit is een werkwijze om overzicht van uitgegeven rechten te creëren en het maakt het gemakkelijker om de juiste rechten toe te kennen. Voor meer informatie over het opstellen van een rechtenmatrix bekijk het thema ‘*rechtenmatrix’* op onze website[[1]](#footnote-1).  Daarnaast bieden we ook twee documenten aan die ondersteuning bieden bij het in- en uitdienstproces van medewerkers. Download deze documenten als je het handig vindt om aan de slag te gaan met het bijhouden van rollen en rechten van de gebruikers in je onderneming.   1. Tool 1 – In- en uit dienst formulier[[2]](#footnote-2) 2. Tool 2 – Overzicht medewerkers[[3]](#footnote-3)   [organisatie] – In- en uit dienst beleid  Your Logo Here  **Doel:**  Dit document (wat kan worden gezien als onderdeel van het *Identity and Access Management (IAM)* ofwel *gebruikersbeheer*)beschrijft de beleidsuitgangspunten ten aanzien van informatiebeveiliging voor een invulling van het in- en uit dienst beleid. In- en uit dienst beleid geeft invulling aan de wijze waarop een organisatie maatregelen treffen voor een adequate inrichting en uitvoering van de autorisatie van nieuwe medewerkers, medewerkers die uit dienst gaan en medewerkers die wijzigingen van rol en/of functie binnen jouw organisatie. Van belang in dit proces is dat alleen bevoegde personen autorisaties toekennen. Het doel van het in-en uit dienst beleid is als volgt:   1. Het inzichtelijk en beheersbaar maken van de medewerkers die rollen en of rechten toegekend krijgen. 2. Het inzichtelijk en beheersbaar maken van medewerkers waarvan rollen en of rechten worden ingetrokken. 3. Het inzichtelijk en beheersbaar maken van medewerkers waarvan rollen en of rechten wijzigen. 4. Het op een zo efficiënt mogelijke wijze doorvoeren van deze medewerkersmutaties met zo min mogelijk verstoringen en om ook veilige toegang tot de juiste bronnen te borgen.   Afbeelding met tekening  Automatisch gegenereerde beschrijvingIn en uit dienst management is gericht op het verminderen van risico’s als gevolg van ongeautoriseerde toegang (met lees en/of schrijfrechten) tot data in systemen en apparaten in een organisatie.  **Scope:** De uitgangspunten opgesteld in dit document gelden voor het leidinggevende/managers en IT werknemers van [organisatie] die toegang hebben tot de systemen en het netwerk van [organisatie], hierbij wordt geen onderscheid gemaakt tussen apparaten van [organisatie] en/of persoonlijke apparaten.  **Definitie van autorisatie:** De bevoegdheden die een gebruiker van een computersysteem heeft om toegang te krijgen tot gegevens of handelingen te mogen uitvoeren. Bijvoorbeeld het opstarten van programma’s of het inzien, wijzigen of wissen van informatie (Cybersecurity Woordenboek, 2019).  **Policy**  Alle medewerkers van [organisatie] spelen een rol als het gaat om het autorisatie tot apparaten en software met als doel het mitigeren van risico’s als gevolg van de bewust of onbewust misbruik hiervan. De mate van verantwoordelijkheid is afhankelijk van de functie van de desbetreffende medewerker.   1. *Leidinggevende*     1. Stel tijdig vast welke rechtenindeling de werknemer toegewezen dient te krijgen bij nieuw in dienst of functiewijziging of welke rechten moet(en) worden verwijderd.    2. Maak in dit proces gebruik van een rechten indeling. Een medewerker kan een rol of meerdere rollen hebben die weer rechten bevat in verschillende systemen of applicatie. Zo heeft iedere rol andere rechten in systemen en applicaties. (denk hiervoor bijvoorbeeld aan de gebruikersrollen ‘Administratie’ en ‘Directie’. Zij zullen beide andere rechten hebben in de verschillende systemen).    3. Als leidinggevende (geautoriseerd voor het doorgeven van personeelswijzigingen aan de IT en HR afdelingen) stel je samen met de betreffende werknemer een in-en uit dienst Afbeelding met tekening        Automatisch gegenereerde beschrijvingformulier op waarvan nieuwe rollen en/of rechten dienen te worden toekend (op basis van de gebruikersrol in je de organisatie) of moeten verwijderd.    4. Dit formulier autoriseren door de leidinggeven en de betreffende medewerker.    5. Het formulier bevat informatie die nodig is voor het toekennen van gebruikersrol(len) en de rechten aan de medewerker voor bepaalde apparaten en/of software. 2. *IT afdeling/applicatiebeheer*    1. Zorg ervoor dat autorisatie verzoeken tijdig (d.m.v. bijvoorbeeld een in- en uit dienst formulier) worden doorgevoerd en de juisten gebruikersrol(len) en rechten worden toegekend aan de nieuwe medewerker in apparaten en software of dat rollen en rechten tijdig worden ingetrokken indien een werknemer wijzigt van functie of uit dienst gaat.    2. Verwerk alleen verzoeken ontvangen van geautoriseerde leidinggevende.   Aldus vastgesteld door de directie van [organisatie] op [datum],  [Naam. Functie] [Naam. Functie]  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
|  |  |

1. Pagina Rechtenmatrix: <https://digitaltrustcenter.nl/rechtenmatrix> [↑](#footnote-ref-1)
2. Template op https://digitaltrustcenter.nl/sites/default/files/2020-06/Formulier%20werknemer%20in-en%20uitdienst.docx [↑](#footnote-ref-2)
3. Template via https://digitaltrustcenter.nl/sites/default/files/2020-06/Template%20Medewerkers%20in-%20en%20uitdienst.xlsx [↑](#footnote-ref-3)