Toegangsbeleid (BASIC)

 Sjabloon

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole**  |  |
| Auteur  |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door  |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie**  | **Datum van goedkeuring** | **Goedgekeurd door**  | **Beschrijving van verandering** |
|  |  |  |  |

# Intro

Binnen **[organisatie]** is toegangsbeheer een essentieel onderdeel van beveiliging dat bepaalt wie toegang heeft tot bepaalde data, applicaties en andere digitale middelen, en onder welke omstandigheden. Dit beleid voor toegangsbeheer beveiligt digitale omgevingen, op dezelfde manier als waarop sleutels en gastenlijsten fysieke ruimten beveiligen. Met andere woorden, ze laten de juiste mensen binnen en houden andere mensen buiten de deur. Dit beleid is gebouwd op technieken zoals verificatie en autorisatie. Deze staan **[organisatie]** toe om te verifiëren dat gebruikers zijn wie ze zeggen dat ze zijn, en dat aan deze gebruikers het juiste toegang is verleend, gebaseerd op context zoals toestel, locatie, functie en nog veel meer.

# Dit beleidsdocument maakt deel uit van een set van beleidsdocumenten die [Organisatie] ondersteunen bij het opstellen van een gedegen strategie rond cyberbeveiliging.

# Toegangsbeheer

**[organisatie]** hanteert het principe van minimale toegang. Dit wil zeggen dat iedere interne of externe gebruiker binnen **[organisatie]** precies voldoende toegang(en) krijgt tot de informatie en systemen die men nodig heeft om hun functie naar behoren uit te voeren. Bovendien verkiest **[organisatie]** standaard Multifactor-authenticatie (MFA) te implementeren en af te dwingen waar mogelijk

De toegang op afstand tot de kritieke en vertrouwelijke systemen van **[organisatie]** vanaf een niet-vertrouwde locatie, zoals het huis van de werknemer of het kantoor van de klant, moet worden beperkt tot de aangewezen gebruikers. De laptops van **[organisatie]** zijn uitgerust met instellingen om een VPN verbinding met de systemen van **[organisatie]** tot stand te brengen.

De toegekende toegangen worden op regelmatige tijdstippen gecontroleerd en indien nodig aangepast. Aanpassingen met betrekking tot toegang, inclusief werken vanop afstand, worden tijdig doorgegeven aan de **[verantwoordelijke binnen de organisatie]** door middel van een Account creation/modificaton fromulier (ACMF) of een account removal formulier (ARF) (**zie ANNEX 1 Formulieren**)

# Accountbeheer

## Gebruikersaccounts

Gebruikersaccounts zijn een veelgebruikte manier om authenticatie te bieden. De volgende regels gelden voor gebruikersaccounts voor toegang tot kritieke en vertrouwelijke systemen:

* moeten uniek en persoonlijk zijn.
* moeten worden beveiligd met een wachtwoord, zoals beschreven in het Wachtwoordbeleid.
* nieuwe gebruikersaccounts voor medewerkers kunnen alleen worden aangevraagd door een bevoegd persoon en worden verwerkt.
* moeten worden ingetrokken wanneer ze verouderd zijn (bijvoorbeeld bij beëindiging van het contract).

## Bevoorrechte accounts

De toewijzing van accounts met privileges (bijv. domeinbeheerder, supergebruiker en root) moet worden beperkt. Bevoorrechte accounts mogen alleen worden gebruikt als geprivilegieerde toegang nodig is. Eigenaars van zulke accounts moeten een niet geprivilegieerde account gebruiken voor normale gebruikersactiviteiten. Systeembeheerders mogen bijvoorbeeld hun account Domeinbeheerder niet gebruiken voor het afhandelen van hun e-mail.

De naam van dit account mag geen informatie over de uitgebreide privileges van het account vrijgeven, dit om misbruik te voorkomen.

Voor bevoorrechte accounts voor kritieke en vertrouwelijke systemen die toegankelijk zijn vanaf niet vertrouwde netwerken zoals het internet, moet multifactor-authenticatie worden gebruikt

## Gedeelde accounts

Het gebruik van gedeelde accounts moet worden voorkomen. Als het redelijkerwijs niet kan worden voorkomen, moet het gebruik van gedeelde accounts worden gecontroleerd. Controles moeten aanwezig zijn voor:

* Weten wie de account kan gebruiken.
* Het gebruik van de account controleren.
* Proces van wachtwoordwijziging en communicatie van het nieuwe wachtwoord.
* Voorkomen van misbruik, bijvoorbeeld bij beëindiging van het contract.

## Accounts voor extern personeel en externe bedrijven

De volgende aanvullende controles moeten worden uitgevoerd voor rekeningen voor extern personeel:

* Accounts moeten gemakkelijk kunnen worden geïdentificeerd als zijnde bestemd voor extern personeel, bijvoorbeeld door een voorvoegsel toe te voegen aan de naam van de account of door het te vermelden in een beschrijving.

Accounts moeten aan het einde van het contract worden ingetrokken. Wanneer dit proces niet volledig kan worden gewaarborgd, moet het account automatisch elke **[3 maanden]** verlopen, tenzij verlenging officieel is goedgekeurd.

## Serviceaccounts voor communicatie tussen systemen

De volgende aanvullende controles moeten aanwezig zijn voor service accounts en accounts voor communicatie van machine naar machine:

* Accounts moeten gemakkelijk geïdentificeerd kunnen worden als een serviceaccount, bijvoorbeeld door een voorvoegsel toe te voegen aan de accountnaam of door het te vermelden in een beschrijving.
* Ook hier geldt het principe van minimale toegang.
* Interactief gebruik van serviceaccounts moet worden voorkomen.

# Authenticatie en autorisatie

**Microsoft Active Directory (AD)** is een centrale authenticatie- en autorisatieoplossing, die toelaat rechten en beveiligingsinstellingen in een netwerk te beheren. AD is geïntegreerd met de Windows-omgeving en biedt de mogelijkheid tot gedelegeerd beheer van de Windowsomgeving van **[organisatie].**

## Authenticatie

* Via een beveiligde verbindingsprocedure moet men de toegang tot systemen en toepassingen kunnen controleren.
* De **[IT-verantwoordelijke]** moet elke poging tot verbinding, ongeacht of deze succesvol is of niet, registreren en monitoren.
* De beginwachtwoorden moeten veilig en rechtstreeks aan de gebruiker worden doorgegeven.
* Deze wachtwoorden zijn zo ingesteld dat men deze direct moet wijzigen.
* Waar passend en uitvoerbaar moet Multifactor-authenticatie worden gebruikt.
* Het gebruikersaccount moet gedurende een vooraf bepaalde periode worden geschorst als de gebruiker een vooraf bepaald aantal mislukte authenticatiepogingen **[3 pogingen]** waagt binnen een vooraf bepaalde periode **[5 minuten].**
* De toegang tot het systeem moet worden opgeschort wanneer het account gedurende een vooraf bepaalde periode **[bijv. 90 dagen]** niet werd gebruikt.

## Autorisatie

* Het verlenen of ontnemen van toegangen tot de informatiesystemen kan enkel tijdig aangevraagd worden via een ACMF / ARF formulier. (zie ANNEX 1 Formulieren)
* Deze toegang kan enkel aangevraagd worden door de HR verantwoordelijke of de N+1 van de betrokkene.
* Vooraleer de toegang wordt verleend, moet **[verantwoordelijke van organisatie]** formeel zijn goedkeuring geven. De **[IT-verantwoordelijke]** moet toegangsrechten verlenen, bijwerken en verwijderen.
* Er wordt zoveel mogelijk gewerkt met autorisatie-groepen en toegang wordt role-based verleend.