Beleid Logische Toegangsbeveiliging

Gemeente Meppel

Inhoudsopgave

Samenvatting

Dit beleidsdocument beschrijft de maatregelen, richtlijnen en procedures die de Gemeente Meppel toepast om de toegang tot gegevens en applicaties te beheren en te beschermen tegen ongeautoriseerde handelingen. Dit beleid is van toepassing op alle informatiesystemen die de gemeente gebruikt, inclusief externe Software-as-a-Service (SaaS) oplossingen. De gemeente voert beveiligingsmaatregelen uit die voortkomen uit de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Het doel is om ervoor te zorgen dat alleen bevoegde personen toegang hebben tot de applicaties. Dit is niet alleen een verplichting om aan wetgeving te voldoen, maar ook essentieel voor het beschermen van de privacy en veiligheid van inwoners en het waarborgen van betrouwbare informatie voor medewerkers. De gemeente streeft ernaar om systemen ondersteunend te maken en overbodige drempels weg te nemen. Dit houdt in dat beveiliging zoveel mogelijk in het ontwerp van informatiesystemen wordt geïntegreerd. Er wordt gebruikgemaakt van een centrale identiteits- en toegangsbeheerservice die voldoet aan strenge eisen, waaronder ondersteuning voor tweefactor- en multifactor-authenticatie, Single Sign-On en gedetailleerde logging van toegangsactiviteiten.

1.Inleiding

Logische toegangsbeveiliging is het geheel aan maatregelen, richtlijnen en procedures die door de gemeente worden toegepast om de toegang tot gegevens en applicaties te beheersen en te beschermen tegen ongeautoriseerde handelingen.

In november 2021 heeft de gemeente het beleid voor logische toegangsbeveiliging vastgesteld. Het voorliggende, nieuwe, beleid voor logische toegangsbeveiliging is een optimalisatie van dit eerder vastgestelde beleid. Door het optimaliseren van het bestaande beleid voor logische toegangsbeveiliging sluit de gemeente aan bij de ontwikkeling van Europese en Nederlandse wetgeving op het gebied van informatiebeveiliging. Ook wordt op deze manier invulling gegeven aan de planning die is opgesteld in het Informatiebeveiligingsplan 2024.

Logische toegangsbeveiliging is geen op zichzelf staand beleid, maar maakt deel uit van het bredere pakket aan informatiebeveiligingsmaatregelen die door de gemeente worden geïmplementeerd. Het heeft veel raakvlakken met fysieke toegangsbeveiliging en daarom zal in 2025 gewerkt worden aan het samenvoegen van deze twee onderwerpen in één beleidsstuk. Bovendien is logische toegangsbeveiliging nauw verbonden met integriteit en het beheer van bedrijfsmiddelen. Medewerkers moeten bij het gebruik van applicaties en andere door de gemeente beschikbaar gestelde bedrijfsmiddelen zoals laptops rekening houden met de uitgangspunten voor logische toegangsbeveiliging die door de gemeente worden gehanteerd.

1.1 Doelstelling

1.1.1 Bedoeling van de vraagstukken centraal

Om de digitale weerbaarheid op orde te krijgen en te houden voert de Gemeente Meppel continu verschillende beveiligingsmaatregelen uit. Deze (verplichte) maatregelen vloeien bijvoorbeeld voort uit de Baseline Informatiebeveiliging Overheid (BIO) en de Algemene Verordening Gegevensbescherming (AVG). Logische toegangsbeveiliging is een van deze beveiligingsmaatregelen. Het doel van de logische toegangsbeveiliging is om te beschrijven welke maatregelen, richtlijnen en procedures de Gemeente Meppel heeft geïmplementeerd om ervoor te zorgen dat uitsluitend bevoegde personen toegang hebben tot gegevens en applicaties.

Logische toegangsbeveiliging is niet alleen een verplichting om te voldoen aan wet- en regelgeving. Het is een essentieel onderdeel van het beschermen van de privacy, veiligheid en belangen van de inwoners van de gemeente. Daarnaast zorgt goede logische toegangsbeveiliging ervoor dat medewerkers van de gemeente toegang hebben tot de juiste en betrouwbare gegevens en applicaties die ze nodig hebben om effectief te werken.

1.1.2 Basis op orde

Gemeenten hebben op basis van wetgeving en bepaalde overeenkomsten toegang tot allerlei externe systemen en toepassingen, zoals BRP, DigiD en Suwinet. Deze wetgeving en overeenkomsten stellen eisen aan beveiligingsmaatregelen die gemeenten dienen te nemen om aan te tonen dat de gemeente risico's binnen haar processen beheerst. Logische toegangsbeveiliging is een van de beheersmaatregelen waar een gemeente op steunt. Gemeenten moeten dan ook in staat zijn om aan te tonen dat ze de basis op orde hebben en de toegangsrechten in een applicatie op een juiste manier zijn geïmplementeerd en worden gecontroleerd.

1.1.3 Systemen ondersteunend maken

Als gemeente doen we ons best om structuren en systemen ondersteunend te maken en overbodige drempels weg te nemen. Voor logische toegangsbeveiliging betekent dit dat we de beveiliging van informatiesystemen zoveel als mogelijk is in het ontwerp te regelen, zonder afbreuk te doen aan de veiligheid ervan. Zowel identiteits- als toegangsbeheer moet zoveel mogelijk op één centrale plek geregeld zijn. In het in 2023 vastgestelde sourcingbeleid staat beschreven dat nieuwe applicaties in de primaire en ondersteunende processen alleen als SaaS (Software-as-a-Service) worden aangeschaft. Om medewerkers toegang te geven tot externe bronnen zoals SaaS-applicaties maken we als gemeente gebruik van een centrale identiteits- en toegangsbeheerservice. Deze service moet aan diverse eisen voldoen om een goede logische toegangsbeveiliging te garanderen en automatisch te kunnen worden uitgerold over verschillende informatiesystemen. Deze eisen omvatten onder andere ondersteuning voor tweefactor- en multifactor-authenticatie, Single Sign-On, en gedetailleerde logging van toegangs- en autorisatieactiviteiten.

1.2 Context en reikwijdte

Logische toegangsbeveiliging is geen op zichzelf staand beleid, maar maakt deel uit van het bredere pakket aan informatiebeveiligingsmaatregelen die door de gemeente worden geïmplementeerd. Het heeft veel raakvlakken met fysieke toegangsbeveiliging en daarom zal in 2025 gewerkt worden aan het samenvoegen van deze twee onderwerpen in één beleidsstuk. Bovendien is logische toegangsbeveiliging nauw verbonden met integriteit en het beheer van bedrijfsmiddelen. Medewerkers moeten bij het gebruik van applicaties en andere door de gemeente beschikbaar gestelde bedrijfsmiddelen rekening houden met de uitgangspunten voor logische toegangsbeveiliging die door de gemeente worden gehanteerd.

Logische toegangsbeveiliging is van toepassing op alle applicaties en gegevens die de Gemeente Meppel gebruikt om haar processen uit te voeren. Ook als applicaties niet op de on-premise voorzieningen van de gemeente draaien is het beleid voor logische toegangsbeveiliging van toepassing, zoals bij het gebruik van Software-as-a-Service (SaaS) oplossingen.

2. Beleidsuitgangspunten

Beleid voor logische toegangsbeveiliging bestaat grofweg uit twee aspecten: toegangsbeheer en identiteitsbeheer. Toegangsbeheer gaat over het definiëren van de rechten en rollen die aan gebruikers worden toegekend. Identiteitsbeheer gaat over dat de juiste gebruikers daadwerkelijk toegang kunnen krijgen tot de informatiesystemen waarvoor ze gemachtigd zijn, door vast te stellen dat de gebruiker is wie die beweert te zijn. Deze twee aspecten staan in nauw verband en zorgen er samen voor dat de toegang tot systemen en gegevens binnen de organisatie veilig en gecontroleerd is.

2.1 Toegangsbeheer

2.1.1 Minimale toegang

Bij het toekennen van toegangsrechten wordt door de gemeente als basis gehanteerd dat de autorisaties van een gebruiker voortkomen uit diens functie of verantwoordelijkheid. De principes die bij toegangsbeheer worden gehanteerd zijn ‘need-to-know’ en ‘need-to-use’. Door gebruikers alleen toegang te geven tot informatie die strikt noodzakelijk is voor hun taken (need-to-know) en tot informatietechnologie en -infrastructuur indien daarvoor een duidelijke noodzaak bestaat (need-to-use) wordt het risico op ongeautoriseerde toegang en misbruik van gegevens en applicaties verminderd, wat bijdraagt aan een betere informatiebeveiliging.

2.1.2 Instroom, doorstroom en uitstroom

Het verstrekken van toegangsrechten gebeurt als medewerkers in dienst treden (instroom), als een medewerker van functie wijzigt (doorstroom), dan wel als medewerkers uit dienst

treden (uitstroom). Dit is vastgelegd in het IDU-proces, de procedure rondom in-, door- en uitstroom. Op basis van de functieprofielen die aan medewerkers worden toegewezen bij in- of doorstroom zijn rollen en rechten voor verschillende applicaties gespecificeerd. De teammanager van de desbetreffende medewerker is verantwoordelijk voor het toekennen van de rollen aan zijn/haar medewerkers, zodat bepaald kan worden tot welke gegevens en applicaties toegang moeten hebben voor het uitvoeren van hun werkzaamheden.

Daarnaast moet de teammanager als informatie-eigenaar ook ervoor zorgen dat de applicatie altijd aansluit op de generieke autorisatieprocedure die door de gemeente gehanteerd wordt zodat medewerkers daadwerkelijk toegang kunnen krijgen tot de gegevens en applicaties die zij nodig hebben voor hun werkzaamheden.

2.1.3 Autorisatiematrix

Elke informatie-eigenaar is verantwoordelijk voor het inzichtelijk maken van de behoeften van gebruikers met betrekking tot toegang tot gegevens en applicaties. Op basis van de geïdentificeerde behoeften worden toegangsrechten toegewezen aan verschillende rollen binnen de applicatie. Dit overzicht is een autorisatiematrix. Op basis van het IDU-proces wordt toegang tot informatie geregeld en de domein-specifieke functieprofielen kunnen gebruikt worden bij het opstellen van een autorisatiematrix binnen de applicatie.

Naast dat de informatie-eigenaar verantwoordelijk is voor het vaststellen van de autorisatiematrix is de informatie-eigenaar ook verantwoordelijk voor het uitvoeren van periodieke controles van de autorisatiematrix. Periodieke controle is noodzakelijk om ervoor te zorgen dat de autorisatiematrix in overeenstemming is met het informatiebeveiligingsbeleid en de vereisten voor gegevensbescherming. De informatie-eigenaar wordt bij het vaststellen en controleren van de autorisatiematrix ondersteund door de functioneel- of applicatie beheerder. De manier waarop deze controle uitgevoerd wordt is beschreven in de procedure rondom autorisatiebeheer en -controle die momenteel in ontwikkeling is.

2.1.4 Functiescheiding

In principe mag geen enkele gebruiker autorisaties hebben om een gehele cyclus van handelingen in een applicatie te beheersen. Het samenbrengen van deze taken bij één gebruiker brengt het risico op belangenconflicten en misbruik van privileges met zich mee. Bij het vaststellen en controleren van de autorisatiematrix is functiescheiding een belangrijk aspect. Geen enkele gebruikersrol mag alle benodigde toegangsrechten hebben om (kritieke) processen volledig te beheren. In plaats daarvan moeten de benodigde toegangsrechten verdeeld worden over meerdere gebruikersrollen, zodat er een scheiding van taken en verantwoordelijkheden ontstaat. Waar nodig wordt tijdens het opstellen van de autorisatiematrix een hulpmiddel, zoals een het opstellen van een conflictmatrix, gebruikt om de scheiding van functies inzichtelijk te maken.

2.1.5 Gebruikerscontrole

Waar de controle van de autorisatiematrix gericht is op het evalueren van toegangsbeheer op een overkoepelend niveau, is de gebruikerscontrole gericht op de operationele aspecten van het beheer van individuele gebruikersaccounts en toegangsrechten binnen het kader van de autorisatiematrix. Gebruikerscontrole beschrijft het beheer van individuele gebruikersaccounts, inclusief het maken, wijzigen en verwijderen van accounts, het toewijzen van specifieke toegangsrechten aan gebruikers en het monitoren van gebruikersactiviteiten. De informatie-eigenaar is verantwoordelijk voor de gebruikerscontrole en wordt hierin ondersteund door de functioneel- en applicatiebeheerders, die verantwoordelijk zijn voor het dagelijks beheer van gebruikersaccounts en toegangsrechten. Ook voor de gebruikerscontrole geldt dat deze uitgevoerd dient te worden conform de procedure autorisatiebeheer en -controle die momenteel ontwikkeld wordt.

2.2 Identiteitsbeheer

2.2.1 Identificatie

In het kader van identiteitsbeheer verwijst identificatie naar het proces waarbij een gebruiker zichzelf bekendmaakt aan een applicatie doormiddel van een unieke identificator, zoals een gebruikersnaam of emailadres. Door gebruik te maken van unieke identificatoren voor elke gebruiker wordt het mogelijk om elke gebruiker te identificeren en zijn activiteiten altijd te herleiden tot één specifieke gebruiker. Om deze reden mag een account ook nooit gedeeld worden met anderen, ook niet tijdens afwezigheid van bepaalde medewerkers. Er worden nooit algemene identificatoren gebruikt, voor herleidbaarheid en transparantie is het namelijk noodzakelijk om te weten welke gebruiker een bepaalde actie heeft uitgevoerd.

2.2.2 Authenticatie

Voor het vaststellen van de identiteit van een gebruiker is het gebruik van enkel een identiteit onvoldoende, de gebruiker moet namelijk ook nog geauthentiseerd worden. Authenticatie is het proces waarbij een informatiesysteem controleert of de gebruiker echt is wie ze beweren te zijn. Single Sign-On (SSO) en twee-factor authenticatie (2FA) zijn de minimaal vereiste verificatiemethoden die door de gemeente gebruikt worden en zijn vastgelegd in het Informatiebeveiligingsbeleid.

2.2.3 Single Sign-On

Single Sign-On (SSO) software zorgt ervoor dat authenticatie tot andere applicaties automatisch verloopt. In plaats van dat gebruikers aparte aanmeldingsgegevens moeten onthouden en invoeren voor elke applicatie die ze gebruiken, maakt SSO het mogelijk om één keer in te loggen en toegang te krijgen tot alle geautoriseerde applicaties zonder opnieuw te worden gevraagd om in te loggen voor elke applicatie. SSO is enkel van toepassing op authenticaties die plaatsvinden binnen de applicaties die gekoppeld zijn aan de centrale identiteits- en toegangsbeheerservice.

2.2.4 Twee-factor authenticatie

In de BIO is vastgelegd dat, als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, dit enkel gebeurt op basis van minimaal twee-factor authenticatie (2FA). 2FA en multi-factor authenticatie (MFA) zijn beveiligingsmethoden die vereisen dat gebruikers niet alleen hun gebruikersnaam en wachtwoord (een aspect van 'iets dat de gebruiker weet') invoeren om toegang te krijgen tot een applicatie, maar ook aanvullende vormen van authenticatie moeten bieden. Deze aanvullende vormen kunnen bestaan uit iets wat de gebruiker bezit, zoals een token of een app op hun smartphone, of uit iets wat de gebruiker ‘is’, zoals een vingerafdruk of gezichtsscan.

2.2.5 Wachtwoord

Een van de vormen van authenticatie die wordt toegepast in MFA en 2FA is het gebruik van iets dat de gebruiker weet. In veel gevallen komt dit neer op het gebruik van een wachtwoord. Voor alle medewerkers van de Gemeente Meppel geldt dat ze een wachtwoord moeten gebruiken dat voldoet aan het op dat moment geldende gemeentelijk wachtwoordbeleid.

3. Hybride werken

Het is momenteel toegestaan om eigen apparaten te gebruiken voor het uitvoeren van taken en gebruiken van gegevens en applicaties. Dit past binnen de technische omgeving en de manier waarop gegevens en applicaties momenteel beschikbaar worden gesteld. Er is echter onvoldoende zicht op de beveiliging van deze privé apparaten, wat aanzienlijke risico’s met zich meebrengt. In het kader van hybride werken, gecombineerd met de verSaaSing van het applicatielandschap, zijn er daarom in dit beleid voor logische toegangsbeveiliging een aantal specifieke kaders opgenomen. Deze kaders worden verder uitgewerkt in het werkplekbeleid en in het beleid voor Mobile Device Management (MDM) die momenteel allebei in ontwikkeling zijn.

3.1 Virtuele desktop

Voor toegang tot gegevens en applicaties van de gemeente wordt momenteel gebruik gemaakt van een virtuele desktop. Bij gebruik van de virtuele desktop ligt de focus van beveiliging vooral op de binnenzijde van het netwerk. De binnenzijde van het netwerk wordt als vertrouwd beschouwd, alles daarbuiten niet. De virtuele desktop wordt daarom ook wel gezien als ‘vertrouwde zone’. De BIO schijft voor dat toegang vanuit een onvertrouwde naar een vertrouwde zone alleen plaats mag vinden op basis van minimaal 2FA. Daarom moet toegang tot de virtuele desktop die momenteel door de gemeente wordt gebruikt altijd gebaseerd zijn op minimaal 2FA.

In 2022 is het sourcingsbeleid vastgesteld, wat inhoudt dat de gemeente in de toekomst afscheid zal nemen van de virtuele desktop in haar huidige vorm. Door de overstap naar SaaS-

applicaties worden steeds minder gegevens lokaal opgeslagen, waardoor een virtuele desktop zoals die nu is ingericht niet meer past bij de toekomstige werkwijze. Dit betekent dat de virtuele desktop in haar huidige vorm in de toekomst losgelaten zal worden.

3.2 Beheerde apparaten

Om medewerkers te faciliteren bij het werken op andere locaties zijn er al een grote hoeveelheid laptops en randapparatuur uitgegeven. Deze apparatuur wordt echter nog niet centraal beheerd door de gemeente, waardoor het ook nog niet als vertrouwd kan worden beschouwd. Wanneer de virtuele desktop in haar huidige vorm in de toekomst wordt losgelaten en medewerkers werken vanuit een ander soort beveiligde omgeving en SaaS-applicaties moeten alle toegangsverzoeken worden geverifieerd, geautoriseerd en versleuteld. Volgens de BIO mogen gebruikers met ongeauthentiseerde apparaten (Bring Your Own Device, BYOD) alleen toegang krijgen tot een onvertrouwde zone. Er wordt momenteel gewerkt aan het centraal beheer van de laptops en een aantal medewerkers werkt al op apparatuur die door de gemeente zelf beschikbaar is gesteld en centraal beheerd wordt (Choose Your Own Device, CYOD).

Door apparaten in een centrale beheeroplossing te registreren en centraal te beheren kan toegang tot gegevens en applicaties op de gemeentelijke apparaten worden beveiligd. Deze centraal beheerde apparaten worden beschouwd als geauthentiseerde apparatuur. Hierdoor kan de gebruiker via deze apparatuur direct toegang krijgen tot de gegevens en applicaties die door de gemeente gebruikt wordt, zonder dat eerst ingelogd hoeft te worden op de huidige virtuele desktop. De manier waarop de gemeente omgaat met het beheer van mobiele apparaten en applicaties zal uitgebreider beschreven worden in het beleid voor Mobile Device Management dat momenteel in ontwikkeling is.

4. Externe toegang

De gemeente kan een externe partij toegang verlenen tot het gemeentelijk netwerk. Het gaat dan bijvoorbeeld om technische ondersteuning die van tijdelijke aard is. Hiervoor dient een procedure gemaakt en gevolgd te worden. Voor externe leveranciers dient er een afweging gemaakt te worden of het strikt noodzakelijk is voor waarborging van dienstverlening om de leverancier toegang te verlenen tot de gemeentelijke infrastructuur vanaf afstand. Externe partijen kunnen niet op eigen initiatief verbinding maken met het besloten netwerk van de gemeente. Daarnaast moet er extra logging en monitoring worden toegepast en dient de gemeente de verbinding te kunnen ontkoppelen indien er verdachte of ongewenste activiteiten worden geconstateerd.

5. Controle en toezicht

Naast de maatregelen die de gemeente neemt in het kader van logische toegangsbeveiliging dient de gemeente ook een controle uit te voeren op de activiteiten van gebruikers binnen informatiesystemen. Dreigingsdetectie en analyse van gebruikersgedrag helpen om aanvallen en datadiefstal proactief tegen te gaan. Daarbij moet zoveel mogelijk geautomatiseerd worden, aangezien het onmogelijk is om alle signalen handmatig te beoordelen. Verdachte en/of ongewenste activiteiten worden, zodra ze zijn geconstateerd, behandeld als beveiligingsincident en opgepakt conform het incidentmanagementproces. Dit houdt in dat zodra er een melding binnenkomt, bijvoorbeeld bij het Servicepunt, via het Serviceportaal, of rechtstreeks bij de CISO of SO, er een impactanalyse wordt uitgevoerd. Op basis van de omvang van het incident worden vervolgens de benodigde stappen genomen.

5.1 Monitoring en response

Een manier om de digitale weerbaarheid te verhogen en te borgen is het inzetten van Monitoring en Response (M&R). M&R houdt in dat digitaal verkeer continu wordt gemonitord om informatiebeveiligingsincidenten te voorkomen, of deze tijdig te detecteren en daar passend op te reageren. M&R sluit aan bij logische toegangsbeveiliging omdat het de gemeente in staat stelt om verdachte en ongewenste activiteiten tijdig te signaleren. Momenteel maakt de gemeente nog geen gebruik van een M&R toepassing. Wel wordt er door de gemeente gewerkt aan het project Monitoring & Response, waarmee de weerbaarheid van de gemeente tegen cyberdreigingen verhoogd wordt. Omdat dit project momenteel al loopt is in dit beleid voor logische toegangsbeveiliging wel rekening gehouden met M&R, bijvoorbeeld door te vereisen dat alle acties van een gebruiker herleidbaar moeten zijn doormiddel van een unieke identificator.

5.2 Logging

Een van de manieren waarop de gemeente achteraf controleert op ongewenste activiteiten die te maken hebben met logische toegangsbeveiliging is logging. Logging is het bijhouden van (log)bestanden die gegevens bevatten over de aard, datum en tijd waarop bepaalde handelingen – waarbij persoonsgegevens worden verwerkt – in een systeem hebben plaatsgevonden. Logging speelt een essentiële rol in het bijhouden van toegangsactiviteiten. In het geval van verdachte of ongewenste activiteit kunnen logbestanden geanalyseerd worden om te achterhalen of ongeautoriseerde toegang heeft plaatsgevonden. Inrichting van logging binnen applicaties en analyse van logbestanden dient te gebeuren conform het gemeentelijk loggingbeleid dat in overeenstemming met het Informatiebeveiligingsplan in Q3 2024 ontwikkeld wordt.

6. Rollen en Verantwoordelijkheden

6.1 College B&W

Het College van Burgemeester en Wethouders (B&W) is integraal (politiek) verantwoordelijk voor de beveiliging van informatie en de borging van de privacy binnen de gemeentelijke bedrijfsprocessen. Hier valt ook het beleid voor logische toegangsbeveiliging onder.

6.2 Directie

De directie is de opdrachtnemer van het college. De directie is verantwoordelijk voor het functioneren van de ambtelijke organisatie in al zijn aspecten, waaronder informatiebeveiliging en privacy. In het kader van logische toegangsbeveiliging en conform het informatiebeveiligingsbeleid zorgt de directie ervoor dat alle processen en systemen en de daarbij behorende middelen altijd onder de verantwoordelijkheid van een teammanager vallen en ziet de directie erop toe dat teammanagers adequate maatregelen nemen om de betrouwbaarheid van informatie te waarborgen.

6.3 Teammanager

Teammanagers spelen een belangrijke rol bij het toepassen van het beleid voor logische toegangsbeveiliging binnen de gemeente. Om deze verantwoordelijkheid te kunnen dragen worden zij ondersteund door bijvoorbeeld de CISO, de PO/SO en functioneel en applicatie beheerders.

Een teammanager kan verschillende rollen hebben, zoals proces-eigenaar, systeem-eigenaar of informatie-eigenaar. Voor logische toegangsbeveiliging is de rol van informatie-eigenaar vooral van belang. Teammanagers zijn proces-eigenaar van de processen die door hun teams uitgevoerd worden en daarmee zijn ze ook informatie-eigenaar van de informatie die bij het uitvoeren van deze processen gebruikt worden. De rol informatie-eigenaar is van belang voor logische toegangsbeveiliging omdat een informatie-eigenaar verantwoordelijk is voor de borging van de beveiliging en integriteit van gegevens. Hieruit volgt dat teammanagers verantwoordelijkheid dragen voor:

- Het vaststellen van de juiste autorisaties voor medewerkers binnen het team.
- Het waarborgen dat medewerkers de juiste toegangsrechten krijgen binnen applicaties waarvoor de teammanager als informatie-eigenaar is gedefinieerd.
- Het (laten) uitvoeren van een controle van de autorisatiematrix en gebruikerscontrole voor applicaties waarvoor de teammanager als informatie-eigenaar is gedefinieerd.

6.4 CISO

De Chief Information Security Officer (CISO) ziet toe op uitvoering van de informatiebeveiligingstaken van de organisatie. De CISO heeft een adviserende en toezichthoudende rol als het gaat om logische toegangsbeveiliging. Hiernaast coördineert en adviseert de CISO ook bij het afhandelen van beveiligingsincidenten.

6.5 Privacy en Security Officer

Zoals is beschreven in het Informatiebeveiligingsbeleid van de Gemeente Meppel is de Privacy en Security Officer (PO/SO) verantwoordelijk voor het opstellen en herijken van beleidsstukken inzake privacy en informatiebeveiliging. Hiernaast adviseert de PO/SO en ziet hij toe of alle maatregelen conform het beleid voor logische toegangsbeveiliging worden toegepast en uitgevoerd. De PO/SO is uitvoerend medewerker op het gebied van privacy en informatiebeveiliging en is daarmee het eerste aanspreekpunt voor de gemeente als het gaat om logische toegangsbeveiliging.

6.6 Functioneel en applicatie beheerders

In het kader van logische toegangsbeveiliging hebben de beheerders vooral een ondersteunende rol richting de teammanagers en informatie-eigenaren. De belangrijkste taken van de functioneel en applicatie beheerders zijn het inrichten, uitvoeren en controleren van de autorisaties en functiescheiding, en het adviseren en ondersteunen van de informatie-eigenaren bij hun verantwoordelijkheden. Daarnaast dragen technisch beheerders zorg voor de technische beveiliging van de gehele infrastructuur, inclusief logische toegangsbeveiliging. In het kader van functiescheiding dient er een apart account te zijn voor beheerswerkzaamheden.

6.7 Gebruikers

Alle medewerkers van de gemeente maken gebruik van gemeentelijke gegevens en applicaties en zijn daarmee verantwoordelijk voor het naleven van beleid voor logische toegangsbeveiliging. Gebruikers moeten zich correct identificeren voordat ze toegang kunnen krijgen tot gegevens en applicaties, ze moeten bijvoorbeeld doormiddel van multi-factor authenticatie bewijzen dat ze geautoriseerd zijn om toegang te krijgen tot specifieke applicaties en gebruikers mogen alleen toegang hebben tot gegevens en applicaties die relevant zijn voor hun werkzaamheden. Hiernaast moeten gebruikers verdachte activiteiten of incidenten die te maken hebben met logische toegangsbeveiliging melden bij de beveiligingsfunctionarissen van de gemeente via het Serviceportaal.

Duurzaamheid in Gemeente Meppel

Gemeente Meppel staat voor duurzaamheid. Dit document is ontworpen voor online gebruik.
Wil je het document toch printen? Print dan in zwart-wit en minimale printkwaliteit.

Kijk voor meer informatie over duurzaamheid in Gemeente Meppel op www.meppel.nl/duurzaam.