

Digitaal toegangsbeleid gemeente Hoorn

November 2021

Versie 1.0

Zaaknummer: 1909332

Inhoud

Inleiding.....	3
Doel 3	
Evaluatie.....	3
Afbakening	3
Definities.....	3
Algemeen beleid	5
Uitgangspunten	5
Wachtwoorden	5
Accounts en toegangsrechten	5
Gebruikersaccount voor systeembeheerders	5
Toegang ICT-dienstverlener	5
Multi factor authenticatie	6
Inloggen op vertrouwde laptops.....	6
Vertrouwde telefoons en/of tablets	6
Zakelijke apps op telefoons en/of tablets.....	6
Vertrouwde en onvertrouwde apparaten	6
Controle op accounts en toegangsrechten	6
Toegang werkgever tot gebruikersaccount.....	7
Organisatie, taken en verantwoordelijkheden	8
Teammanager	8
Teammanager I&A	8
Gebruikers	8
Data- of applicatie eigenaar	8
Coördinator informatiebeveiliging.....	8
Functionaris informatiebeveiliging.....	8

Inleiding

Digitale toegang is een belangrijk onderdeel van de gemeentelijke informatiebeveiliging. Een goede digitale toegang zorgt ervoor dat onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatie.

Doel

Het doel van dit beleid is het creëren van een duidelijk handelingskader als het gaat om digitale toegang.

Evaluatie

Het beleid wordt jaarlijks geëvalueerd en indien nodig geactualiseerd.

Afbakening

Dit beleid is van toepassing op alle informatiesystemen waar wij (in)direct gebruik van maken. Het geldt ook wanneer informatiesystemen technisch niet binnen de gemeente draaien, bijvoorbeeld bij SaaS-applicaties. Dit beleid geldt voor iedereen die gebruik maakt van de informatiesystemen van de organisatie.

Definities

Onvertrouwde zone: Dit is de zone waarbinnen veiligheidsmaatregelen worden toegepast. De organisatie beschouwt alle werklocaties als een onvertrouwde zone. Op deze locaties worden gegevens verwerkt die vertrouwelijk of bedrijfsgevoelig kunnen zijn. Het is nodig om maatregelen te treffen die ervoor zorgen dat deze gegevens voldoende beveiligd zijn.

Vertrouwd apparaat: Laptop/ telefoon of tablet die eigendom is van de organisatie of een eigen apparaat zoals een Choose your own device

(CYOD). De gebruiker geeft toestemming dat deze beheerd mag worden door de organisatie.

Onvertrouwd apparaat: Alle overige laptops/ telefoons of tablets die niet beheerd worden door de organisatie.

Multi factor authenticatie (MFA): Een gebruiker doorloopt twee stappen om toegang tot gemeentelijke informatie te krijgen. De gebruiker combineert bij deze twee stappen iets dat hij/zij heeft met iets dat hij/zij weet. De eerste stap is gebruikersnaam en wachtwoord. De tweede stap is het ingeven van een tweede sleutel om in te kunnen loggen. Dit is een gegeneerde code die een gebruiker via een authenticator app ontvangt en invoert. Het kan ook het vertrouwde apparaat zijn van de organisatie. Alleen deze combinatie zorgt ervoor dat je toegang krijgt.

Informatiesysteem: applicaties, informatiesystemen, hardwarecomponenten, de gebruikersdatabases van het ICT-netwerk.

Wachtwoord: Een wachtwoord is een reeks tekens waarmee toegang wordt verkregen tot informatie, een computer of een mobile device. Een wachtwoord is altijd toegewezen aan een gebruikersnaam die een fysieke gebruikers uniek identificeert.

Mobile device management (MDM):

Met Mobile Device Management (MDM) beheer je mobiele apparaten zoals smartphones, tablets en laptops vanuit een centrale beheerportal. Via de beheerportal kun je regels afdwingen op de apparaten die in de MDM omgeving zijn opgenomen. Een voorbeeld daarvan is het op afstand vergrendelen en/of wissen bij verlies of diefstal van het device.

Data- of applicatie eigenaar Er is altijd één eigenaar van een applicatie of data dashboard. Dit is de medewerker die verantwoordelijk is over het betreffende bedrijfsproces. In de organisatie is dat vaak een teammanager. Per applicatie of data dashboard wordt een eigenaar vastgelegd in het registratiesysteem van team I&A. Voor algemene software worden ook eigenaren vastgelegd.

Biometrische gegevens: Zijn lichamelijke kenmerken die kunnen worden gebruikt om individuele personen te identificeren. Het lezen van vingerafdrukken, gezichtsafbeeldingen of retinascans zijn hier voorbeelden van.

Algemeen beleid

Uitgangspunten

Digitale toegang tot een informatiesysteem van de organisatie vindt altijd plaats in de onvertrouwde zone. Dit betekent dat onderstaande uitgangspunten op elke locatie gelden. Hierdoor zijn er geen locaties met lagere veiligheidseisen en is er geen verschil in de werking van de werkplek en veiligheid op de verschillende werklocaties en/of thuis.

Wachtwoorden

1. Standaard wachtwoorden van informatiesystemen worden gewijzigd, voordat een informatiesysteem in gebruik genomen wordt.
2. Wachtwoorden worden op een veilige manier uitgegeven. Er vindt een controle plaats op de identiteit van de gebruiker.
3. Tijdelijke wachtwoorden hebben een geldigheidsduur die niet langer is dan één werkdag en moeten bij het eerste gebruik worden gewijzigd.
4. Wachtwoorden zijn alleen bij de gebruiker bekend.
5. Wachtwoorden bestaan uit minimaal 8 vrij te kiezen karakters en zijn complex van samenstelling.
6. Wachtwoorden zijn maximaal een jaar geldig als het informatiesysteem voldoet aan het digitaal toegangsbeleid. In een informatiesysteem die geen MFA ondersteunt wordt het wachtwoord minimaal elk half jaar vernieuwd.
7. Gebruikers worden ondersteund in het beheren van hun wachtwoorden door het beschikbaar stellen van een wachtwoordenkuis.
8. Het inloggen met biometrische gegevens is toegestaan.
9. Het wachtwoord wordt niet getoond op het scherm tijdens het ingeven.

Accounts en toegangsrechten

10. Een gebruikersaccount is persoonsgebonden en mag alleen door die persoon worden gebruikt.
11. Na beëindiging van het dienstverband worden de toegangsrechten verwijderd.
12. Na wijziging van het dienstverband of de functie worden de toegangsrechten aangepast naar de rechten passen bij de nieuwe functie.
13. Inactieve accounts worden na 90 dagen geblokkeerd
14. Er is een sluitende formele registratie-, wijziging- en afmeldprocedure voor het beheren van gebruikers en toegangsrechten.
15. Rolgebaseerd wordt toegang verleend tot systemen en informatie. Uitzonderingen worden gemotiveerd vastgelegd.
16. Toegangsrechten van gebruikers kunnen uitsluitend worden aangevraagd door de verantwoordelijk leidinggevende.
17. Accounts voor meerdere personen (groepsaccounts) is niet toegestaan, tenzij dit wordt gemotiveerd en vastgelegd door de proceseigenaar. Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven. Dit is vastgelegd in een autorisatiematrix.

Gebruikersaccount voor systeembeheerders

18. Al het bovenstaande is van toepassing
19. Bij het toepassen van een gebruikersaccount voor systeembeheerders is MFA verplicht. Als hiervan wordt afgeweken omdat dit technisch niet mogelijk is dan is dit vastgelegd.
20. Bij een succesvol inlogproces door een systeembeheerder wordt de datum en tijd van de voorgaande inlogpoging getoond.

Toegang ICT-dienstverlener

21. Bij een overeenkomst met een ICT-dienstverlener worden eisen aan informatiebeveiliging, inclusief autorisatiebeheer en omgang met persoonsgegevens vastgelegd.

- 22. Een ICT-dienstverlener die voor ondersteuning toegang nodig heeft, krijgt tijdelijke toegang, op afspraak, met een gebruikersaccount. Dit mag een algemeen, niet persoonlijk account zijn. Na afronding van het werk wordt de toegang direct geblokkeerd.
- 23. Er is een procedure aanwezig voor toegang van een ICT-dienstverlener
- 24. Het inloggen door een ICT-dienstverlener wordt vastgelegd.

Multi factor authenticatie

- 25. Voor toegang tot het informatiesysteem is MFA verplicht.
- 26. Bij het gebruik van MFA is er de voorkeur voor de authenticator app boven een MFA mogelijkheid middels SMS.
- 27. Het in bezit hebben van een vertrouwd apparaat, is een eerste factor. In dit geval is gebruikersnaam/wachtwoord dus voldoende om aan te melden.

Inloggen op vertrouwde laptops

- 28. Als voor een gebruikersnaam drie keer een foutief wachtwoord gegeven is, wordt het account minimaal 15 minuten geblokkeerd. Als er geen lock-out periode ingesteld kan worden, dan wordt het account geblokkeerd totdat de gebruiker hiervoor een verzoek indient via de servicedesk.

Vertrouwde telefoons en/of tablets

- 29. De wachtwoordinstellingen worden automatisch door een MDM systeem afgedwongen.
- 30. Het wachtwoord (of pincode) voor toegang tot het mobiele apparaat moet bestaan uit minimaal 6 karakters.
- 31. Inloggen met biometrische gegevens is toegestaan.
- 32. Na 90 dagen inactiviteit worden bedrijfsgelateerde apps verwijderd.
- 33. Het aantal foutieve inlogpogingen staat op maximaal 10 keer. Daarna worden bedrijfsgelateerde apps verwijderden de fabrieksinstellingen terug gezet.

- 34. Het is mogelijk om een vertrouwd mobiel apparaat op afstand te wissen bij verlies of diefstal.

Zakelijke apps op telefoons en/of tablets

- 35. Informatie van de organisatie wordt uitsluitend beschikbaar gesteld in zakelijk, door de organisatie goedgekeurde apps.
- 36. In geval van nieuwe zakelijke app wordt data-classificatie toegepast en een beveiligingstoets uitgevoerd. Als er persoonsgegevens worden verwerkt in de app wordt privacy by design toegepast.
- 37. Informatie in zakelijke apps is alleen binnen de zakelijke app beschikbaar. Er is geen interactie met andere apps of het besturingssysteem van de telefoon of tablet. Uitzonderingen hierop is de camera van de telefoon of tablet. Is een uitzondering op deze regel noodzakelijk voor een app dan wordt privacy by design en een beveiligingstoets toegepast.
- 38. Zodra een medewerker uit dienst gaat, is bedrijfsinformatie niet meer beschikbaar en toegankelijk in de zakelijke apps.

Vertrouwde en onvertrouwde apparaten

- 39. Met een vertrouwd apparaat is er geen verschil tussen het werken thuis en/of op kantoor.
- 40. Met een onvertrouwd apparaat is toegang tot informatie van de organisatie beperkt tot webapplicaties, zoals Office365 en intranet.

Controle op accounts en toegangsrechten

- 41. Periodiek worden controles gedaan naar juistheid en rechtmatigheid van de accounts en toegangsrechten. De resultaten worden vastgelegd in een rapportage. Bevindingen worden geregistreerd als incident en worden hersteld conform dit beleid.
- 42. Per kwartaal worden accounts voor systeembeheerders gecontroleerd. De resultaten worden vastgelegd in een rapportage.

Bevindingen worden geregistreerd als incident en worden hersteld conform dit beleid.

Toegang werkgever tot gebruikersaccount

43. Alleen een leidinggevende kan toegang krijgen tot een gebruikersaccount van een medewerker. De aanvraag wordt voor advies voorgelegd aan de functionaris gegevensbescherming. Gevoelige en risicovolle aanvragen kunnen aan de directie worden voorgelegd ter goedkeuring. In de aanvraag is het zwaarwegend belang van de toegang, de noodzaak en de duur aantoonbaar gemotiveerd. Deze registratie wordt vastgelegd in het personeelsdossier en indien mogelijk vooraf bekend gemaakt aan de medewerker.
44. Er kijkt altijd een tweede onafhankelijke persoon mee als er toegang wordt verleend aan de teammanager tot een gebruikersaccount of mailbox.

Organisatie, taken en verantwoordelijkheden

In dit hoofdstuk zijn de taken en verantwoordelijkheden beschreven.

Teammanager

- Vraagt toegangsrechten aan en zorgt dat een gebruiker alleen toegang heeft tot wat noodzakelijk is voor de functie. Uitsluitend verantwoordelijk leidinggevend, zoals teammanagers en concernmanagers, zijn bevoegd om deze aanvragen te doen.
- Geeft wijzigingen en beëindigen van een functie of taken die gevolgen hebben voor de rechten en/of toegang tijdig en volledig door via geldende procedures.
- Is verantwoordelijk voor een correcte gebruikersdatabase en zorgt er hiermee voor dat informatie alleen kan worden verwerkt door geautoriseerde gebruikers.

Teammanager I&A

- Zorgt voor procedures die nodig zijn om dit beleid uit te kunnen voeren.
- Zorgt voor monitoring om de juistheid van de gebruikersdatabase van het ICT-netwerk van de organisatie te borgen. Dit betekent dat er, in samenwerking met team HR, een sluitende administratie van de gebruikersdatabase binnen de organisatie is.

Gebruikers

- Geven bij verlies of diefstal van telefoon, laptop of tablet dit direct aan de servicedesk door
- Zijn op de hoogte dat wachtwoorden persoonsgebonden zijn en niet mogen worden gedeeld.

Data- of applicatie eigenaar

- Geeft op basis van een rol of functie een gebruiker toegang tot een informatiesysteem of deel van een informatiesysteem.
- Zorgt voor periodieke controles, zodat juistheid en rechtmatigheid van accounts en toegangsrechten geborgd is.
- Zorgt voor het in stand houden van de beveiliging in overeenstemming met de gestelde eisen.

Coördinator informatiebeveiliging

- Zorgt voor het opzetten, invoeren en monitoren van dit beleid.
- Zorgt ervoor dat er in samenwerking met de functionaris informatiebeveiliging een jaarlijkse evaluatie is van het digitale toegangsbeleid en dat op basis van nieuwe wet- en regelgeving, mogelijkheden en risico's het beleid wordt bijgesteld.
- Zorgt voor bewustzijn over informatieveiligheid en hiermee het digitale toegangsbeleid binnen de organisatie. Werkt hiervoor nauw samen met de functionaris informatiebeveiliging.

Functionaris informatiebeveiliging

- Houdt toezicht op de naleving van dit beleid. En rapporteert hierover aan de directie.
- Adviseert over eisen aan informatiebeveiliging, gebruikerstoegang en beveiligingsmaatregelen

Gemeente Hoorn

Nieuwe Steen 1

Postbus 603

1620 AR Hoorn

T 0229 25 22 00

www.hoorn.nl

