nationale ombudsman

Vertrouwelijk

Toegangsbeveiligingsbeleid

Nationale ombudsman

Document classificatie

Vertrouwelijk

Referenten documenten:

- ISO/IEC: 27002:2017 hoofdstuk 9, toegangsbeveiliging
- Baseline Informatiebeveiliging Overheid 2019 versie 1.4
- Informatiebeveiligingsbeleid Nationale ombudsman
- Wachtwoordenbeleid Nationale ombudsman

Versiebeheer

Versienummer	1.0
Gemaakt door	Matthijs Kerkvliet
Goedgekeurd door	
Datum eerste versie	15 oktober 2020
Laatst bijgewerkt	17 september 2021

Geschiedenis wijzigingen

Datum	Versie	Aangepast door	Beschrijving van de wijziging
24-03-21	0.2	Martijn de Bruin	Review
14-04-21	0.3	Rion Rijker	Review & Update
26-04-2021	0.4	Matthijs Kerkvliet	Review en update
29-04-21	0.5	Martijn de Bruin	Review en update
08-07-21	0.6	Matthijs Kerkvliet	Review en aanpassing procesverantwoordelijke

26-07-21	0.7	Rion Rijker	Review en update.
30-7-2021	0.7.1	Rion Rijker	Update op basis van gezamenlijke review
17-09-2021	1.0	Matthijs Kerkvliet	Versie na vaststelling BVO

Inhoud

1 Inleiding

Dit document beschrijft de uitgangspunten van de Nationale ombudsman over toegang tot informatiesystemen, maar ook toegang tot fysieke ruimten.

1.1 Uitgangspunten voor toegangsbeveiliging

Het basisprincipe is dat toegang tot alle informatiesystemen, netwerken, diensten en informatie verboden is, tenzij uitdrukkelijk toestemming is verleend aan afzonderlijke gebruikers of groepen van gebruikers. Er moet een procedure voor gebruikersregistratie voor elk informatiesysteem en dienst zijn.

Toegang tot alle fysieke gebieden in de organisatie is niet toegestaan, behalve de publieke gebieden. Via het autorisatiesysteem wordt toegang verleend tot fysieke ruimten in het gebouw. Dit beleid specificeert regels voor toegang tot informatiesystemen, diensten en inrichtingen, terwijl het beleid voor Geclassificeerde Informatie regels definieert voor toegang tot afzonderlijk documenten en registraties.

Het voorgaande vertaalt zich in de volgende uitgangspunten:

- **Need-to-know**: Medewerkers krijgen alleen toegang tot informatie die zij nodig hebben voor het uitvoeren van de betreffende taken en/of rollen.
- **Need-to-use**: Medewerkers krijgen alleen toegang tot informatie verwerkende faciliteiten die noodzakelijk zijn voor de uitvoering van de betreffende taken en/of rollen.

1.2 Inrichting van toegangsbeveiliging

De inrichting van het identiteit- en toegangsbeheer is vastgelegd in een toegangsbeveiligingsarchitectuur[1]. Binnen de No worden toegangsrechten gekoppeld aan de rol die een medewerker heeft.

Het doel van dit document is om regels voor toegang op verschillende systemen, apparatuur, inrichtingen en informatie te definiëren, gebaseerd op bedrijfs- en beveiligingseisen voor toegang. Dit document is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS), d.w.z. zowel voor alle informatie- en communicatietechnologie, als ook voor de documentatie binnen het toepassingsgebied. Gebruikers van dit document zijn werknemers van Nationale ombudsman. Dit beleid is van toepassing op iedereen binnen de No.

[1] Ten tijde van de totstandkoming van het toegangsbeveiligingsbeleid was deze toegangsbeveiligingsarchitectuur nog niet gereed en in gebruik.

1.3 Leeswijzer

Hoofdstuk twee beschrijft de beleidsregels voor toegangsbeveiliging. In hoofdstuk drie staan de verantwoordelijkheden van de betrokken functionarissen beschreven. Hoofdstuk vier beschrijft waar de registratie van toegekende autorisaties en de controle daarop wordt vastgelegd. In hoofdstuk vijf wordt beschreven met welke frequentie de systeemeigenaar de toegekende autorisaties beoordeelt.

2 Beleidsregels voor toegangsbeveiliging

De volgende regels gelden binnen de No voor toegangsbeveiliging.

1. Groepen informatiediensten, gebruikers en informatiesystemen dienen binnen het netwerk gescheiden te worden, om de kans op onbevoegde toegang tot gegevens te minimaliseren.
2. De taken, verantwoordelijkheden en bevoegdheden worden vastgelegd in een autorisatiematrix (overzicht van autorisatiebevoegden). Deze matrix wordt op basis van de uitgangspunten in dit hoofdstuk beoordeeld door de proces / applicatie eigenaar.
3. Toegang van functioneel-, systeem- en applicatiebeheerders tot informatiesystemen wordt gelogd en deze logs worden periodiek geëvalueerd door de CISO.
4. Waar uitvoerend personeel nooit toegang mag hebben tot beheersystemen van de Nationale ombudsman, zal ondersteunend personeel geen directe toegang hebben tot informatiesystemen waarin gegevens (klachten/dossiers) van burgers worden verwerkt (tenzij de uitvoering van hun functie dat vereist).
5. Er is een sluitende formele registratie- en afmeldprocedure voor alle gebruikers.
6. De procedures beschrijven alle fasen van de levenscyclus van de gebruikerstoegang en de relaties tussen de autorisatieprocessen (van eerste registratie tot en met de beëindiging).
7. Het gebruiken van niet-gepersonaliseerde accounts is niet toegestaan vanwege herleidbaarheid en transparantie, tenzij dit wordt gemotiveerd en vastgelegd door de systeemeigenaar.
8. Toegang tot informatiesystemen door gebruikers en infrastructuurcomponenten, wordt gereguleerd door het toegangsmechanisme (i) gebruikersidentificatie (zoals een gebruikersaccount) en (ii) authenticatie (zoals een wachtwoord).
9. 'Role-based-access': Gebruikers worden op basis van juiste functierollen (en/of autorisatieprofielen) door de applicatie- / systeem- / proceseigenaar of projectleider geautoriseerd voor het gebruik van applicaties of gegevens.
10. Toegang tot informatiesystemen wordt uitsluitend verleend na autorisatie door een bevoegde functionaris.
11. Een actueel mandaatregister (autorisatiematrix) is aanwezig in het ISMS, waaruit blijkt welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.
12. Toegang tot het netwerk door leveranciers wordt beperkt tot alleen de noodzakelijke toegang voor de uitvoering van taken of werkzaamheden.
13. Met externen/ leveranciers worden in een (raam-)overeenkomst afspraken gemaakt over toegang tot vertrouwelijke (persoons-)gegevens of fysieke toegang tot ruimten waar vertrouwelijke gegevens worden verwerkt.

14. De FG en de CISO maken een risicoafweging indien een externe/ leverancier waarmee geen (raam-)overeenkomst is afgesloten toegang tot (persoons-)gegevens of een fysieke toegang ruimt waarin vertrouwelijke gegevens worden verwerkt nodig heeft.
15. Als vanuit een niet-vertrouwde zone toegang wordt verleend naar een vertrouwde zone, dan gebeurt dit in lijn met het wachtwoordenbeleid en daar waar mogelijk minimaal op basis van 2-factor authenticatie.
16. Beheerders dienen gebruik te maken van een wachtwoordkluis met minimaal twee factor authenticatie. Als geen gebruik wordt gemaakt van twee factor authenticatie, dan gelden de eisen zoals gesteld in het wachtwoordenbeleid.

3 Verantwoordelijkheden

Om de toegangsbeveiliging binnen de No te borgen zijn verschillende rollen benodigd. Het is hierbij van belang dat de personen met deze rollen zich bewust zijn van hun verantwoordelijkheden en hiernaar handelen.

3.1 Procesverantwoordelijke

De procesverantwoordelijke is er voor verantwoordelijk dat de juiste autorisaties zijn vastgesteld per rol. Dit gebeurt in een autorisatiematrix. Op basis van deze autorisatiematrix kan vervolgens de systeemeigenaar de autorisaties toekennen voor de applicatie waar de systeemeigenaar verantwoordelijk voor is. De procesverantwoordelijke is er voor verantwoordelijk dat de toegekende autorisaties in de autorisatiematrix in lijn zijn met de classificatie van het informatiesysteem en de daarin verwerkte gegevens.

3.2 Helpdesk

De Helpdesk[2] is verantwoordelijk voor het op verzoek van een systeemeigenaar verlenen, intrekken of aanpassen van toegangsrechten en stelt eisen aan een autorisatieproces, dat bestaat uit enkele sub-processen zoals: toekennen (of verlenen), verwerken, intrekken, blokkeren, archiveren en controleren. Dit autorisatieproces zorgt ervoor dat autorisaties gestructureerd plaatsvinden.

De helpdesk is daarnaast verantwoordelijk voor het beoordelen van autorisatieverzoeken. De helpdesk beoordeelt de ontvangen verzoeken op basis van onderstaande criteria.

a. De aanvraag of het wijzigingsverzoek is volledig en op de juiste manier ingevuld.
b. De aanvrager is overeenkomstig het mandaatregister bevoegd om toegangsrechten aan te vragen.

[2] In sommige gevallen doet de functioneel beheerder dit.

3.3 Systeemeigenaar

De systeemeigenaar is eindverantwoordelijk voor het aanvragen van toegangsrechten en het borgen dat alleen de daartoe gerechtigde medewerkers toegang krijgen. De functioneel beheerder voert het toekennen van toegang uit.

De aanvraag wordt gestart doordat de aanvrager – of de manager van de aanvrager – het hiervoor bestemde formulier (sjabloon) in de servicemanagementapplicatie invult of e-mailt naar de helpdesk. Dit verzoek wordt vervolgens door de helpdesk behandeld. Het verzoek bevat minimaal de volgende gegevens:

a) naam aanvrager (deze wordt in de huidige servicemanagementapplicatie automatisch ingevuld),
b) gebruiker/begunstigde,
c) aanvraagdatum (de huidige servicemanagementapplicatie vult automatisch de datum van het versturen van de aanvraag in),
d) gewenste ingangsdatum,
e) einddatum (bij tijdelijke medewerkers),
f) gewenste bevoegdheden.

Bij beëindigen van dienstverband worden toegangsrechten tot informatie en informatie verwerkende faciliteiten ingetrokken. Wanneer een medewerker binnen de organisatie van functie verandert dienen toegangsrechten overeenkomstig te worden aangepast. Dit wordt geregeld via een procedure die beschrijft:

a) wanneer en hoe een gebruiker wordt afgemeld. Bijvoorbeeld in verband met een andere functie, pensioen, andere werkgever of ontslag;
b) wie verantwoordelijk is voor het intrekken van gebruikers-ID's en toegangsrechten;
c) door wie en hoe de gebruikers-ID en toegangsrechten uit het informatiesysteem worden verwijderd, en;
d) waar, hoe en hoelang dit in de administratie dient te worden vastgelegd. Bijvoorbeeld tot 3 maanden na intrekking van de bevoegdheden, een wettelijke bewaartermijn of de bewaartermijn van de auditlogging, zodat je kunt zien wie bevoegd was.

De systeemeigenaar is verantwoordelijk om de actuele stand van zaken van de toegekende autorisaties te controleren. Deze controle vindt plaats op geldigheid en rechtmatigheid van de verstrekte actuele autorisaties (medewerkers, gebruikersnamen, bevoegdheden).

De resultaten van iedere periodieke controle legt de helpdesk/ functioneel beheer voor aan de procesverantwoordelijken. Bij akkoord worden deze rapportages ter controle voorgelegd aan de CISO. Deze rapportage dient van de volgende onderdelen te zijn voorzien:

- Wie heeft de controle uitgevoerd?
    - De volledige naam, functie en voorzien van een (herleidbare) handtekening/paraaf
- Resultaten van de controle, die kan bestaan uit:
    - Autorisatie overzichten (voorzien van een productiedatum)
    - Een controledatum
    - De conclusie van de controle
- Aanbevelingen

Tijdens deze controle stelt de controleur vast dat de door de procesverantwoordelijke vastgestelde actuele autorisatiematrix in overeenstemming is met het, door de systeemeigenaar verstrekte, overzicht van autorisaties. De CISO rapporteert opvallende zaken in zijn/ haar kwartaalrapportage.

3.4 Projectleider

De projectleider is verantwoordelijk voor het aanvragen van toegangsrechten voor externen /leveranciers die toegang tot de No systemen vereisen. De projectleider is tevens verantwoordelijk voor het informeren van deze partijen over de binnen de No geldende informatiebeveiliging- en privacyvereisten.

Indien de leverancier / externe toegang tot persoonsgegevens verkrijgt of tot een BBN2 of hoger geclassificeerd informatiesysteem dan wordt voor het verlenen van toegang samen met de FG en/of CISO een risicoafweging gemaakt.

3.5 Gebruikers

In het geval dat gebruikers authenticatie-informatie ontvangen voor het verlenen van toegang tot informatiesystemen behoren gebruikers hier vertrouwelijk mee om te gaan. Om dit te borgen dienen gebruikers zich aan de volgende richtlijnen te houden:

- Door ondertekening van het integriteitsbeleid, accepteren gebruikers eveneens de verplichting om wachtwoorden vertrouwelijk te houden, zoals voorgeschreven door dit document.
- Elke gebruiker kan en mag alleen een persoonlijke en unieke toegewezen gebruikersnaam gebruiken.
- Elke gebruiker heeft de optie om een eigen wachtwoord te kiezen, waar dit van toepassing is.

3.6 CIO

De Chief Information Officer (CIO) is eindverantwoordelijk voor het bestaan van een mandaatregister (autorisatiematrix) binnen de organisatie. De matrix bevat welke personen bevoegdheden hebben voor het verlenen van toegangsrechten dan wel functieprofielen.

3.7 CISO

De Chief Information Security Officer (CISO) is verantwoordelijk voor het periodiek controleren van de juiste uitvoering van dit beleid. Daarnaast is de CISO verantwoordelijk voor het beoordelen van de door de systeemeigenaar uitgevoerde risico-assessment over toegang van externen / leveranciers tot BBN2 en hoger geclassificeerde systemen /applicaties.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de volgende criteria in ogenschouw te worden genomen:

- aantal incidenten in verband met ongeautoriseerde toegang tot informatie
- vertraagde wijziging van toegangsrechten in geval van wijziging of beëindiging van het dienstverband/contract
- aantal en toedracht informatiesystemen waarop dit toegangsbeveiligingsbeleid niet is toegepast
- mate waarin is afgeweken van de in dit document benoemde verantwoordelijkheden voor toegangsbeveiliging

3.8 FG

De FG is verantwoordelijk voor het voor het beoordelen van de door de systeemeigenaar uitgevoerde risico-assessment over toegang van externen/ leveranciers tot informatiesystemen /applicaties die persoonsgegevens bevatten.

4 Beoordeling

Systeemeigenaren dienen, met de volgende intervallen, te beoordelen of de verleende toegangsrechten nog steeds in overeenstemming zijn met de bedrijfs- en beveiligingseisen:

BBN niveau	***Intervallen voor regelmatige beoordeling***
1	Minimaal 1x per jaar
2	Elk half jaar
3	Elk Kwartaal

Het resultaat van deze controle wordt overeenkomstig bovenstaande tabel gerapporteerd in het BVO.