[logo organisatie]

[naam organisatie]

Comment [DK1]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

TOEGANGSBELEID

Code:	
Versie:	
Versiedatum	
Gemaakt door:	
Goedgekeurd door:	
Classificatie:	

Comment [DK2]: De documentcodering moet in overeenstemming zijn met het bestaande organisatiecoderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

Versieblad

Datum	Versie	Gemaakt door	Omschrijving van de aanpassing
DD/MM/JJJJ	0.1	Dejan Kosutic	Concept Basisdocument

Inhoudsopgave

1. DOEL, TOEPASSINGSGEBIED EN GEBRUIKERS 3

2. GEREFEREERDE DOCUMENTEN 3

3. TOEGANGSCONTROLE 3

3.1. INTRODUCTIE 3
3.2. GEBRUIKERSPROFIEL A 3
3.3. GEBRUIKERSPROFIEL B 4
3.4. RECHTENBEHEER 4
3.5. REGELMATIGE BEOORDELING VAN TOEGANGRECHTEN 5
3.6. WIJZIGING VAN STATUS OF BEEÏNDIGING VAN CONTRACT 5
3.7. TECHNISCHE IMPLEMENTATIE 6
3.8. WACHTWOORDENBEHEER 6

4. REGISTRATIEBEHEER OP BASIS VAN DIT DOCUMENT 7

5. GELDIGHEID EN DOCUMENTBEHEER 7

1. Doel, toepassingsgebied en gebruikers

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 [naam organisatie].

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules A.9.1.1, A.9.1.2, A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.5, A.9.2.6., A.9.3.1, A.9.4.1, A.9.4.3
- Informatiebeveiligingsbeleid
- Verklaring van Toepasselijkheid
- [Beleid voor Geclassificeerde Informatie]
- [Verklaring van Goedkeuring van ISMS Documenten]
- [Lijst van Wet-, Regelgeving, Contractuele en Andere Verplichtingen]

Comment [DK3]: Indien u niet een dergelijke lijst heeft, neem dan in deze lijst alle wetgeving en contracten op die vereisten bevatten voor toegangscontrole.

3. Toegangscontrole

3.1. Introductie

Het basisprincipe is dat toegang tot alle systemen, 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 systeem en dienst zijn.

Comment [D4]: Verwijder dit hele item indien beheersmaatregel A.9.2.1 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

Toegang tot alle fysieke gebieden in de organisatie is toegestaan, behalve de gebieden voor welke rechten dienen te worden verleend door de geautoriseerde persoon (item "Rechtenbeheer").

Dit Beleid specificeert regels voor toegang tot systemen, diensten en inrichtingen, terwijl het Beleid voor Geclassificeerde Informatie regels definieert voor toegang tot afzonderlijk documenten en registraties.

Comment [D5]: Te verwijderen indien het Beleid voor Geclassificeerde Informatie niet is opgelegd

3.2. Gebruikersprofiel A

Comment [D6]: Pas aan het standaard beheersgebied van de organisatie aan.

Gebruikersprofiel A heeft de volgende toegangsrechten:

Naam van systeem /netwerk/ dienst	Gebruikersrechten

Comment [D7]: Kan gespecificeerd zijn op het niveau van het gehele systeem of een enkele module.

Comment [D8]: Specificeer of ze leesrechten, schrijven, bewerken, verwijderen of uitvoer- of specifieke functies bevatten.

De volgende functies hebben toegangsrechten volgens Gebruikersprofiel A:

- [functie 1]
- [functie 2]

Comment [D9]: Vermeld alle functies. Het kan [illegible] gedurende het dienstverband.

3.3. Gebruikersprofiel B

Comment [D10]: Extra gebruikers-profielen worden vermeld op de wijze zoals in dit item.

Gebruikersprofiel B heeft de volgende toegangsrechten:

Naam van systeem /dienst	[illegible]

Comment [D11]: Kan gespecificeerd zijn op het [illegible] module.

Comment [D12]: Specificeer of ze leesrechten, [illegible] specifieke functies bevatten.

De volgende functies hebben toegangsrechten volgens Gebruikersprofiel B:

- [functie 1]
- [functie 2]

3.4. Rechtenbeheer

Comment [D13]: Verwijder dit hele item indien beheersmaatregel A.9.3.2 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

Rechten aangaande de hierboven genoemde gebruikersprofielen (verlenen of verwijderen toegangsrechten) worden op de volgende manier: toegewezen

Comment [DK14]: Deze tabel kan worden [illegible] eigenaren.

Naam systeem / netwerk/ [illegible]	[illegible] ***toegangsrechten***	***Vorm van autorisatieproces***

Comment [D15]: Door e-mail, schriftelijk besluit, mondeling, via het systeem, enz. – bij voorkeur moet ere en registratie zijn.

Bij het toewijzen van rechten dient de verantwoordelijke zowel de bedrijfs- en beveiligingseisen voor toegang mee te nemen (gedefinieerd in de risicobeoordeling), als ook de classificatie van informatie welke wordt benaderd met dergelijke toegangsrechten, in overeenstemming met het Beleid Geclassificeerde Informatie.

3.5. Regelmatige beoordeling van toegangrechten

Comment [D16]: Verwijder dit hele item indien beheersmaatregel A.9.2.5 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

Eigenaren van een systeem en eigenaren van inrichtingen voor wie speciale rechten vereist zijn, dienen, met de volgende intervallen, beoordeeld te worden of de verleende toegangsrechten nog steeds in overeenstemming zijn met de bedrijfs- en beveiligingseisen:

Comment [D17]: Pas aan, indien noodzakelijk.

Naam van system/ netwerk/ dienst/ fusiek gebied	**Intervallen voor regelmatige beoordeling**

Comment [D18]: De frequentie dient te worden gedefinieerd, daarbij rekening houdend met het belang van risico verbonden met het systeem gebaseerd op de resultaten uit de risicobeoordeling.

Elke beoordeling moet worden vastgelegd [specificeer hoe de registraties worden bewaard].

Comment [D19]: Een formulier, formeel rapport, handgeschreven notities, enz. kunnen worden gebruikt.

3.6. Wijziging van status of beeïndiging van contract

Comment [D20]: Verwijder dit hele item indien beheersmaatregel A.9.2.6 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

Bij wijziging in dienstverband of beëindiging ervan, dient [functie] direct de verantwoordelijke die de rechten heeft verleend aan de werknemer in kwestie in te lichten.

Bij wijziging van contractuele relaties met externe partijen die toegang hebben tot systemen, diensten en inrichtingen, of bij afloop van het contract, contracteigenaar dient direct de verantwoordelijke die rechten heeft verleend aan de externe partijen in kwestie in te lichten.

De toegangsrechten voor alle personen van wie van de status van hun dienstverband of de contractuele relatie is gewijzigd, dient direct te worden verwijderd of gewijzigd door de verantwoordelijk als gedefinieerd in de volgende paragraaf

3.7. Technische implementatie

De technische implementatie van de toewijzing of verwijdering van toegangsrechten wordt door de volgende personen uitgevoerd:

[illegible] ***netwerk/ dienst/ fysiek*** [illegible]	[illegible]

In deze tabel vermelde personen mogen niet vrijelijk toegangsrechten verlenen of verwijderen, maar [illegible] voor toewijzing van rechten.

3.8. Wachtwoordenbeheer

Wanneer gebruikerswachtwoorden worden toegewezen en gebruikt, dan dienen de volgende regels in acht te worden genomen:

- door ondertekening van de Verklaring van Goedkeuring van ISMS Documenten, accepteren [illegible]
- [illegible]
- elke gebruiker heeft de optie om zijn/haar eigen wachtwoord te kiezen, waar van toepassing
- het tijdelijk gebruikte wachtwoord voor de eerste inlog op het systeem dient uniek en sterk [illegible]
- [illegible] wijze en gebruikersidentiteit dient van te voren te worden gecontroleerd
- het wachtwoordbeheersysteem dient te vereisen van de gebruiker het tijdelijke [illegible]
- [illegible] gebruiker te vereisen
- het wachtwoordenbeheersysteem dient te vereisen dat de gebruikers om de drie maanden [illegible]
- [illegible] wachtwoordenbeheersysteem de identiteit van de gebruiker te bepalen door [specificeer hoe]

Comment [D21]: Verwijder dit item indien het [illegible] bestaat.

Comment [D22]: Pas deze regels aan volgens de beoordeelde risico's.

Comment [DK23]: Afzonderlijke regels kunnen [illegible]

Comment [D24]: Meer details kunnen hier worden gegeven.

Comment [D25]: Bijv. door verzending van een [illegible] enz.

- de gebruiker dient de ontvangst van het wachtwoord te bevestigen door [specificeer hoe]
- [illegible]
- [illegible] dient het systeem het gebruikersaccount in kwestie te blokkeren
- [illegible] gewijzigd tijdens de initiële installatie
- bestanden die wachtwoorden bevatten dienen apart van de systeemgegevens van de [illegible]

Comment [D26]: Bijv. door in te loggen op het [illegible]

4. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
[Registraties van toegewezen rechten (in elektronische vorm- e-mail bericht)]	[naam intranetmap]	[functie verantwoordelijk voor de technische implementatie]	Registraties kunnen niet worden bewerkt; alleen [functie] heeft het recht om dergelijke registraties op te slaan	Registraties worden opgeslagen voor 3 jaar
[Registraties van reguliere beoordeling van toegangsrechten]	Computer van [functie], [naam van de archiefmap/-kast]	[functie]	Alleen [functie] heeft toegangsrechten tot dergelijke registraties	Registraties worden opgeslagen voor 3 jaar

Comment [D27]: Pas aan naar wat van toepassing is.

Comment [D28]: Pas aan naar wat van toepassing is.

Alleen [functie] kan andere werknemers rechten tot de hierboven genoemde documenten verlenen.

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. Hij/zij dient het document te controleren en indien nodig [illegible].

Comment [DK29]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

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

- [illegible] toegang tot informatie
- vertraagde wijziging van toegangsrechten in geval van wijziging of beëindiging van het [illegible]

- aantal systemen niet in dit document inbegrepen
- [illegible] document

[functie]
[naam]

_____
[handtekening]

Comment [DK30]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.