[logo organisatie]

[naam organisatie]

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

BELEID VOOR BEVEILIGDE ONTWIKKELING

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. BEVEILIGDE ONTWIKKELING EN ONDERHOUD 3

3.1. RISICOBEOORDELING TEN BEHOEVE VAN HET ONTWIKKELINGSPROCES 3
3.2. BEVEILIGEN VAN DE ONTWIKKELINGSOMGEVING 3
3.3. TOEGEPASTE BEVEILIGINGSPRINCIPES 3
3.4. BEVEILIGINGSEISEN 4
3.5. BEVEILIGINGSEISEN GERELATEERD NAAR PUBLIEKE NETWERKEN 4
3.6. CONTROLEREN EN TESTEN VAN HET IMPLEMENTEREN VAN DE BEVEILIGINGSEISEN 4
3.7. OPSLAGSYSTEEM 4
3.8. VERSIEBEHEER 4
3.9. WIJZIGINGSBEHEER 4
3.10. BESCHERMING VAN TESTGEGEVENS 5
3.11. BENODIGDE BEVEILIGINGSTRAINING 5

4. REGISTRATIEBEHEER OP BASIS VAN DIT DOCUMENT 5

5. GELDIGHEID EN DOCUMENTBEHEER 5

6. BIJLAGE 6

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is om de basisregels voor veilig ontwikkeling van software en systemen te definiëren.

Dit document is van toepassing op de ontwikkeling en onderhoud van alle diensten, architectuur, software en systemen welke onderdeel zijn van het Managementsysteem voor Informatiebeveiliging (ISMS).

Gebruikers van dit document zijn alle werknemers van [naam organisatie] welke werkzaam zijn op gebied van ontwikkeling en onderhoud.

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules A.14.1.2, A.14.1.3,A.14.2.1, A14.2.2, A.14.2.5, A.14.2.6, A.14.2.7, A.14.2.8, A.14.2.9, A.14.3.1
- Methodologie voor Risicobeoordeling en Risicobehandeling
- Beveiligingsbeleid Leveranciers
- [Beleid voor Wijzigingsbeheer]/[Bedieningsprocedures voor de Beheersing van Informatie en Communicatie Technologie]
- Plan voor Training en Bewustzijn

Comment [DK3]: Kies welke van deze twee documenten u gaat gebruiken.

3. Beveiligde ontwikkeling en onderhoud

Comment [DK4]: Omdat de technologie welke gebruikt word erg verschilt van organisatie tot organisatie, zult u deze sectie moeten aanpassen aan uw specifieke omstandigheden.

3.1. Risicobeoordeling ten behoeve van het ontwikkelingsproces

Buiten het feit dat de risicobeoordeling wordt uitgevoerd conform de Methode van [illegible] punten uitvoeren:

Comment [DK5]: [illegible] specificeer hoe vaak.

- [illegible]
- het risico in relatie tot onbevoegde veranderingen tot de ontwikkelingsomgeving
- [illegible]
- het risico dat nieuwe technologie mogelijk met zich mee brengt indien het gebruikt wordt in de organisatie

3.2. Beveiligen van de ontwikkelingsomgeving

Comment [DK6]: Verwijder deze sectie indien beheersmaatregel A.14.2.6 niet van toepassing is.

[identificeer zowel intern als extern de vereisten, beschrijf hier hoe de toegang tot de [illegible] gescheiden van de test- en productie omgeving en hoe back-ups worden gemaakt].

3.3. Toegepaste beveiligingsprincipes

Comment [DK7]: Verwijder deze sectie indien beheersmaatregel A.14.2.5 niet van toepassing is.

[Functie] zal procedures uitvaardigen voor het beveiligd bouwen van een informatiesysteem, zowel voor ontwikkeling van nieuwe systemen en voor het onderhoud van de bestaande systemen, naast het stellen van de minimale standaarden welke moeten worden nageleefd.

Dezelfde toegepaste beveiligingsprincipes kunnen worden toegepast op uitbestede ontwikkeling, en gedefinieerd worden door de contracten als aangegeven in [Beveiligingsbeleid Leveranciers].

3.4. Beveiligingseisen

Wanneer nieuwe informatiesystemen verworven worden of bestaande systemen worden ontwikkeld of veranderd, dan moet [functie] beveiligingseisen vastleggen in de Specificatie van Eisen voor Beveiliging (zie bijlage).

3.5. Beveiligingseisen gerelateerd naar publieke netwerken

[Functie] is verantwoordelijk voor het definiëren van beveiligingsmaatregelen in relatie tot applicatieve diensten welke over het publieke netwerk gaan:

- de beschrijving van welke authenticatiesystemen dienen te worden gebruikt
- de beschrijving van hoe vertrouwelijkheid en integriteit van informatie veilig gesteld wordt
- de beschrijving hoe de onweerlegbaarheid van maatregelen zeker gesteld wordt

[Functie] is verantwoordelijk voor het definiëren van maatregelen voor online transacties welke onderstaande moeten bevatten:

- hoe foutieve routering voorkomen zal worden
- hoe het verzenden van incomplete gegevens voorkomen zal worden
- hoe niet geautoriseerde wijzigingen in berichten voorkomen zal worden
- hoe niet geautoriseerde duplicatie van berichten voorkomen zal worden
- hoe niet geautoriseerde onthulling van gegevens voorkomen zal worden

3.6. Controleren en testen van het implementeren van de beveiligingseisen

[Functie] is verantwoordelijk om de methodologie, verantwoordelijkheden en het tijdstip van verificatie te definiëren omgaande of alle aan beveiligingsvereisten van de Specificaties van Eisen voor Beveiliging zijn voldaan, en omgaande of het systeem acceptabel is voor productie.

3.7. Opslagsysteem

[Beschrijf hier waar de code en alle andere bestanden gerelateerd aan de ontwikkeling worden bewaard, en hoe ze worden beveiligd tegen ongeautoriseerde toegang en ongeautoriseerde wijzigingen]

3.8. Versiebeheer

[Beschrijf hier wat het systeem van versiebeheer is (nummering, data, enz.) en hoe het wordt opgelegd in uw ontwikkelingsomgeving]

3.9. Wijzigingsbeheer

Comment [DK8]: Bijv. richtlijn voor beveiligde programmeertechnieken (apart voor iedere programmeertaal), gedocumenteerde technieken, veilige versie maatregel, data validatie, enz.

Omvat alle architecturale lagen-zaken, gegevens, applicaties en technologie.

Comment [DK9]: Verwijder deze paragraaf indien beheersmaatregel A.14.2.7 niet van toepassing is.

Comment [DK10]: Verwijder deze sectie indien beheersmaatregel A.14.1.1 niet van toepassing is.

Comment [DK11]: Als alternatief kunt u dit als een taak toevoegen aan een projectplan, of iets van dien aard.

Comment [DK12]: Verwijder deze sectie indien beheersmaatregel A.14.1.2 en A.14.1.3 niet van toepassing zijn.

Comment [DK13]: Maatregelen mogen bevatten, digitale handtekening, encryptie, identificatie en authenticatiesystemen, etc. Toepassen van maatregelen moeten conform wet- en regelgeving zijn.

Comment [DK14]: Verwijder deze sectie indien beheersmaatregel A.14.2.8 en A.14.2.9 niet van toepassing zijn.

Comment [DK15]: B.v. test inputs en verwachte outputs, code analyse tools of kwetsbaarheid scanners.

Dit moet gedaan worden in een realistische testomgeving.

Comment [DK16]: Goede praktijk is om de testen uit te voeren wanneer de ontwikkeling is afgerond door het ontwikkelingsteam, en door een onafhankelijk team.

Comment [DK17]: Niet alleen de finale test wanneer de ontwikkeling is afgerond, maar ook gedurende het hele ontwikkelingsproces.

Comment [DK18]: Verwijder de gedeelte als beheersmaatregel A.14.2.2 en A.14.2.4 niet van toepassing worden geacht.

Wijzigingen in de ontwikkeling en gedurende het onderhoud van de systemen dient te worden gedaan volgens [Beleid voor Wijzigingbeheer]/[Bedieningsprocedures voor de Beheersing van Informatie en Communicatie Technologie]

Comment [DK19]: Kies welke van deze documenten u zult gaan gebruiken.

3.10. Bescherming van testgegevens

Comment [DK20]: Verwijder de gedeelte als beheersmaatregel A.14.3.1 niet van toepassing worden geacht.

Vertrouwelijke gegevens, als ook gegevens die kunnen worden gerelateerd aan individuele personen dienen niet te worden gebruikt als testgegevens. Uitzonderingen kunnen worden goedgekeurd door [Functie], in welk geval [Functie] dient de definitieve hoe deze testgegevens worden beveiligd.

3.11. Benodigde beveiligingstraining

[Functie] bepaalt het niveau van beveiligingscompetenties en kennis benodigd voor het ontwikkelingsproces en stelt de training voor aan [Functie]. [Functie] neemt de relevante trainingen op in het Plan voor Training en Bewustzijn.

4. Registratiebeheer op basis van dit document

Naam registratie	*Opslaglocatie*	*Persoon verantwoordelijk voor opslag*	*Beveiligingsmaatregelen voor registraties*	*Bewaartermijn*
[Lijst van risico gerelateerd aan het ontwikkelings-proces	Computer van [functie]	[functie]	[alleen functie mag deze bestanden benaderen]	3 jaar voor de lijsten die niet meer geldig zijn
[Procedures voor het beveiligd bouwen van informatie-systemen]	[intranet organiatie]	[functie]	[alleen functie mag deze bestanden publiceren en bewerken]	3 jaar voor de lijsten die niet meer geldig zijn
[Testplannen]	[intranet organiatie]	[functie]	[alleen functie mag deze bestanden publiceren en bewerken]	3 jaar voor de lijsten die niet meer geldig zijn

Comment [DK21]: Pas de periode in deze kolom aan naar uw specifieke behoeften.

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 het minstens één keer per jaar bij te werken.

Comment [DK22]: Dit is slechts een aanbeveling, pas regelmatig aan indien van toepassing.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de [illegible] in ogenschouw te worden genomen:

- [illegible] beveiligingsmaatregelen in de systemen gebouwd

6. Bijlage

- Specificatie van Eisen voor Beveiliging

[functie]
[voor- en achternaam]

_____
[handtekening]

Comment [DK23]: Alleen noodzakelijk indien de Procedure voor Beheersing van Documenten en Registraties voorschrijft dat papieren documenten moeten worden ondertekend.