[logo organisatie]

[naam organisatie]

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

BELEID VOOR INFORMATIE-OVERDRACHT

Comment [DK2]: Dit Beleid hoeft niet in een apart document te worden beschreven indien dezelfde regels zijn voorgeschreven door de Procedures voor Beheersing van de Informatie en Communicatie Technologie.

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

Comment [DK3]: 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

Het doel van dit document is om de beveiliging van de informatie en software die wordt uitgewisseld binnen of buiten de organisatie te waarborgen.

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 [organisatorisch eenheid voor informatie- en communicatietechnologie].

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules A.13.2.1, A.13.2.2
- Informatiebeveiligingsbeleid
- [Beleid voor Geclassificeerde Informatie]
- [Beveiligingsbeleid Leveranciers]

3. Overdracht van informatie

3.1. Elektronische communicatiekanalen

De informatie van de organisatie mag worden uitgewisseld via de volgende elektronische communicatiekanalen: e-mail, download van bestanden van het internet, overdracht van gegevens via [geef namen van gespecialiseerde communicatiesystemen], telefoons, faxmachines, sms-berichten, draagbare media, en forums en sociale netwerken.

[Functie] bepaalt de communicatiekanalen die kunnen worden gebruikt voor elk type van informatie, en mogelijke beperkingen aangaande toestemmingen voor het gebruik van communicatiekanalen, d.w.z. welke activiteiten zijn verboden.

Bovenop de maatregelen voorgeschreven in het Beleid voor Geclassificeerde Informatie schrijft [functie] extra maatregelen voor elk type gegevens en communicatiekanalen voor, gebaseerd op de resultaten van de risicobeoordeling.

3.2. Relaties met externe partijen

Externe partijen zijn verschillende dienstverleners, bedrijven voor onderhoud van hardware and software, bedrijven voor behandelen van transacties of gegevensverwerking, klanten, enz.

Om informatie en/of software uit te wisselen met enige externe partij, dient een overeenkomst te worden ondertekend, wat de verantwoordelijkheid is van [functie]. De overeenkomst kan in papieren of elektronische vorm bestaan (bijv. Overeengekomen algemene voorwaarden en condities) en dient

Comment [DK4]: Verwijder dit item indien beheersmaatregel A.13.2.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK5]: De media in kwestie kan worden gespecificeerd.

Comment [DK6]: De forums en sociale netwerken in kwestie kunnen worden gespecificeerd.

Comment [DK7]: Voeg toe of verwijder [communicatiekanalen in overeenstemming met de risicobeoordeling en de kanalen die normaal in de organisatie worden gebruikt.

Comment [DK8]: Deze tekst kan worden vervangen door [het type gegevens en communicatiekanalen, beperkingen en verboden] activiteiten voor te schrijven.

Comment [DK9]: [Is annotatie als dit item] niet bestaat.

Comment [DK10]: Verwijder dit item indien beheersmaatregel A.13.2.2 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

clausules te bevatten die in lijn zijn met de risicobeoordeling), en dient ten minste het volgende te bevatten:

- methode van identificatie van de andere partij
- autorisatie voor het benaderen van de informatie
- waarborgen van onweerlegbaarheid
- technische standaarden voor gegevensoverdracht
- incidentenopvang
- labeling en behandeling van gevoelige informatie
- copyright

Overeenkomsten met externe partijen dienen te worden opgetekend volgens het [Beveiligingsbeleid Leveranciers]

4. Registratiebeheer op basis van dit document

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
[Besluiten over de voor specifieke types, beperkingen, verboden activiteiten van informatie gebruikte communicatiekanalen] - elektronische vorm	[naam intranetmap]	[functie]	Eenmaal gecreëerd, kan de registratie vervolgens niet worden gewijzigd	3 jaar

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 eens per jaar bij te werken.

Comment [DK11]: 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:

- aantal van gebruikte communicatiekanalen in strijd met dit document
- aantal van externe partijen met welke informatie wordt uitgewisseld zonder een getekende overeenkomst
- aantal bedrijfsinformatiesystemen die informatie uitwisselt zonder gespecificeerde beveiligingsmaatregelen

[functie]
[naam]

_____
[handtekening]

Comment [DK12]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.