Comment [DK1]: Om meer te leren over back-ips te beheren. Lees dit artikel: Backup policy – How to determine backup frequency http://www.iso27001standard.com/blog/2013/05/07/backup-policy-how-to-determine-backup-frequency/

[logo organisatie]

Comment [DK2]: Alle velden in dit document gemarkeerd met spekhaken [ ] moeten worden ingevuld.

[naam organisatie]

BEDIENINGSPROCEDURES VOOR BEHEERSING VAN DE INFORMATIE EN COMMUNICATIE TECHNOLOGIE

Comment [DK3]: Delen van dit document dat gedetailleerder dienen te worden gespecificeerd, kan als een apart document (beleid/procedures) worden opgesteld.

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

Comment [DK4]: 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 het correct en veilig functioneren van de informatie- en communicatietechnologie 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 gerelateerde documentatie binnen het toepassingsgebied.

Gebruikers van dit document zijn werknemers van [organisatorisch eenheid voor informatie- en communicatietechnologie].

2. Gerefereerde documenten

- ISO/IEC 27001 norm, A.8.3.2, A.11.2.7, A.12.1.1, A.12.1.2, A.12.3.1, A.12.4.1, A.12.4.3, A.13.1.1, A.13.1.2, A .13.2.1, A.13.2.2, A.14.2.4
- Informatiebeveiligingsbeleid
- [Bedrijfscontinuïteitstrategie]
- [Beleid ten aanzien van het Gebruik van Netwerkdiensten]
- [Beleid voor Draagbare Apparaten en Telewerken]
- [Beleid voor Geclassificeerde Informatie]
- [Inventarisatie van Bedrijfsmiddelen]
- [Beveiligingsbeleid Leveranciers]

3. Procedures voor Informatie en Communicatie Technologie

3.1. Wijzigingsbeheer

Elke wijziging aan operationele of productiesystemen dient op de volgende manier te worden gemaakt:

1. De wijziging mag worden voorgesteld door [specificeer functies]
2. De wijziging dient te worden geautoriseerd door [functie], die de rechtvaardiging voor het [illegible]
3. [illegible]
4. [functie] is verantwoordelijk voor de controle dat de wijziging is geïmplementeerd in overeenstemming met het vereiste
5. [illegible] het systeem kan in productie worden gebracht alvorens een grondige test is uitgevoerd
6. implementatie van wijzigingen dient te worden gerapporteerd aan de volgende personen: [illegible]

Comment [DK5]: Verwijder dit hele item indien beheersmaatrege A.12.1.2 is als niet van toepassing is aangegeven in de Verklaring van Toepasselijkheid.

Comment [DK6]: Verwijder dit item indien het Beleid voor Wijzigingsbeheer in een apart document is neergelegd.

Comment [DK7]: Het kan gespecificeerd zijn [illegible] driverupdate, installatie van patches, configuratiewijzigingen, enz.

Comment [DK8]: Andere manier van het [illegible] de stappen uitvoert en dat er dus geen definitie van de verantwoordelijke in elke stap nodig is.

De wijzigingsregistratie worden bewaard [geef de naam van het formulier, of beschrijf een andere methode van registreren wijzigingen]

3.2. Back-up

3.2.1. Back-up procedure

Back-up kopieën dienen voor alle systemen te worden geïdentificeerd in de [Bedrijfscontinuïteitstrategie] en met de frequentie in dat document.

[Functie] is verantwoordelijk voor het proces voor het maken van reservekopieën (back-up), software en systeemimages. [Indien noodzakelijk, beschrijf de gebruikte technologie voor het maken van de back-up, specificeer verantwoordelijkheden voor afzonderlijke activiteiten, locaties voor de opslag van back-up kopieën, fysieke beveiliging voor back-up kopieën, encryptie, wachtwoorden, enz.]

Logbestanden van het back-up proces worden automatisch gecreëerd op systemen waar de back-up kopie wordt gemaakt.

3.2.2. Testen van back-up kopieën

Back-up kopieën en het proces van het gegevensherstel dient te worden getest en wel minstens [één keer in de drie maanden] door het proces voor het herstel van gegevens te implementeren op [identificeer de server waar het herstel van de gegevens wordt uitgevoerd], en controleren dat alle gegevens succesvol zijn hersteld.

[Functie] is verantwoordelijk voor het testen van back-up kopieën. Registraties over het testen van back-up kopieën worden bewaard [beschrijf het registratieformulier – op papier of in elektronische vorm, is er een voorgeschreven formulier, enz.].

3.3. Beveiligingsbeheer voor het netwerk

[Functie] is verantwoordelijk voor het beheer en beheersen van het computernetwerk, zowel voor het waarborgen van de informatiebeveiliging in netwerken als ook voor het beveiligen van de aan het netwerk verbonden diensten tegen onbevoegde toegang. Het is daarom noodzakelijk:

- de operationele verantwoordelijk voor netwerken te scheiden van de verantwoordelijkheid voor gevoelige applicaties en andere systemen
- de gevoelige gegevens passerend over het publieke netwerk te beveiligen door [beschrijf de gebruikte technologie voor de beveiliging en specificeer de verantwoordelijkheden en de verantwoordelijken]
- de gevoelige gegevens passerend over het draadloze netwerk te beveiligen door [beschrijf de gebruikte technologie voor de beveiliging en specificeer de verantwoordelijkheden en de verantwoordelijken]
- de apparatuur verbonden aan het netwerk vanaf externe locaties te beveiligen door [beschrijf de gebruikte technologie voor de beveiliging en specificeer de verantwoordelijkheden en de verantwoordelijken]

Comment [DK9]: Verwijder dit item indien beheersmaatregel A.12.3.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK10]: Verwijder dit item indien het Beleid voor Back-up.

Comment [DK11]: In geval date en dergelijk document niet bestaat, dan dienen alle systemen die een back-up vereisen hier vermeld te worden met de back-upfrequentie.

Comment [DK12]: Back-up kopieën moeten op voldoende locaties worden opgeslagen om gevolg ing van de hoofdlocatie onder deze niet wordt gemaakt bij een ramp.

Comment [DK13]: Pas de frequentie aan in overeenstemming met de beoordeelde risico´s.

Comment [DK14]: Verwijder dit item indien beheersmaatregel A.13.1.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK15]: Of refereer aan het Beleid voor en Telewerken.

- Om inkomend verkeer van draagbare apparaten te scheiden, installeer een unieke firewall regels [beleid] op, statische routes, Virtuele Local Area Networks (VLAN), enz.
- de beschikbaarheid van de netwerkdiensten te waarborgen door [beschrijf maatregelen welke beschikbaarheid waarborgen]
- [functie] dient regelmatig te controleren en geïmplementeerde maatregelen te testen

[Functie] dient beveiligingsfuncties het niveau van verwachte diensten voor alle netwerkdiensten definiëren ongeacht of deze diensten intern of extern worden geleverd – indien mogelijk, dienen dergelijke vereisten vastgelegd te worden met de leveranciers van de diensten.

De toegang tot netwerkdiensten wordt voorgeschreven door het Beleid ten aanzien van het Gebruik van Netwerkdiensten.

3.4. Netwerkdiensten

[Functie] dient beveiligingsfuncties en het niveau van de verwachte diensten voor alle netwerken te definiëren, ongeacht of deze diensten in huis of uitbesteed worden verzorgd – dergelijke vereisten dienen te worden vastgelegd met leveranciers van diensten.

Indien de netwerkdiensten zijn uitbesteed, dan dienen de vereisten in een overeenkomst te worden vastgelegd in het [Beveiligingsbeleid Leveranciers].

3.5. Verwijdering en vernietiging van apparatuur en media

Alle gegevens en erkende software opgeslagen op draagbare opslagmedia (bijv. op CD, DVD, USB flash drive, memory card, enz., maar ook op papier) en op alle apparatuur met opslagmedia (bijv. computers, mobiele telefoons, enz.) dient te worden verwijderd of het medium te worden vernietigd voordat het wordt weggegooid of hergebruikt

De verantwoordelijke voor het verwijderen van gegevens/ vernietiging van media dient de eigenaar van het bedrijfsmiddel in kwestie over de verwijdering/vernietiging in te lichten. De eigenaar van het bedrijfsmiddel dient de Lijst van Bedrijfsmiddelen te vernieuwen.

3.5.1. Apparatuur

[Functie] is verantwoordelijk voor controle en verwijdering van gegevens van apparatuur, tenzij het Beleid voor Geclassificeerde Informatie anders voorschrijft. Gegevens dienen te worden verwijderd [beschrijf de gebruikte technologie voor het verwijderen van gegevens van media in de apparatuur], maar indien het proces niet veilig genoeg is rekening houdend met de gevoeligheid van de gegevens, dan dient het opslagmedium te worden vernietigd.

3.5.2. Draagbare opslagmedia

[Functie] is verantwoordelijk voor de verwijdering van gegevens van draagbare opslagmedia, tenzij het Beleid voor Geclassificeerde Informatie anders voorschrijft. Gegevens dienen te worden verwijderd [beschrijf de gebruikte technologie voor het verwijderen van gegevens van de media],

Comment [DK16]: De frequentie kan worden gespecificeerd – d.w.z. elke dag, of op bepaalde dagen van de maand, enz.

Comment [DK17]: Maatregelen kunnen worden gespecificeerd – d.w.z. firewall, intrusion detection systemen, enz.

Comment [DK18]: Verwijder dit item indien beheersmaatregelen A.8.3.2 en A.11.2.7 zijn aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK19]: Verwijder dit document [indien Beleid voor Verwijdering en Vernietiging als een apart document vormt.

Comment [DK20]: Het kan verder worden [verklaard dat dit opslag in eigen organisatie handelaar wordt overdracht naar een andere organisatie (bijv. door verkoop, donatie, verzending voor reparatie, enz.)

Comment [DK21]: Het kan verder worden verklaard dat dit betekend dat het aan een andere gebruiker is gegeven, enz.

Comment [DK22]: Verwijder dit item indien beheersmaatregel A.8.1.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK23]: Te verwijderen indien een dergelijk beleid niet bestaat.

Comment [DK24]: Bijv. Lijst van [gespecificeerde tools die gebruikt dienen te worden, specificeer of het hier het proces van overschrijven met nullen is gebruikt.

Comment [DK25]: Dit kan zijn bijv. een harde schijf van de server.

Comment [DK26]: [Te verwijderen als een dergelijk beleid niet bestaat.

maar indien het verwijderingproces niet veilig genoeg is in relatie tot de gevoeligheid van de gegevens, dan dient het opslagmedium te worden vernietigd.

3.5.3. Papieren media

Werknemers van de organisatie die afzonderlijke documenten behandelen zijn verantwoordelijk voor de vernietiging van papieren media, lees het Beleid voor Geclassificeerde Informatie anders voorschrijft. Papieren media worden vernietigd door papiervernipperaars.

3.5.4. Verwijdering- en vernietigingsregistraties; commissie voor destructie van gegevens

Registraties van verwijdering/vernietiging moeten voor alle als "Beperkt" en "Vertrouwelijk" geclassificeerde gegevens worden bewaard. Registraties dienen de volgende informatie te bevatten: informatie over de media, datum van verwijdering/vernietiging, methode van verwijdering/vernietiging, en de persoon die het proces heeft uitgevoerd.

Alle als "Vertrouwelijk" geclassificeerde informatie dient te worden verwijderd/vernietigd in de aanwezigheid van een commissie bestaande uit geautoriseerde personen voor wat betreft de informatie in kwestie.

3.6. Informatie-overdracht

3.6.1. Elektronische communicatiekanalen

De informatie van de organisatie kan worden uitgewisseld via de volgende elektronische communicatiekanalen: e-mail, download van bestanden van het internet, overdracht van gegevens via (geef namen van gespecialiseerde communicatie systemen), telefoons, faxmachines, sms-berichten, draagbare, 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.

3.6.2. 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 clausules te bevatten in lijn met de risicobeoordeling), en dient tenminste het volgende te bevatten:

- methode van identificatie van de andere partij

Comment [DK27]: Te verwijderen als een dergelijk beleid niet bestaat.

Comment [DK28]: Of specificeer een andere technologie.

Comment [DK29]: Pas aan het classificatieniveau van de organisatie aan.

Comment [DK30]: Verwijder dit item indien het beleid voor Informatie-overdracht een apart document vormt.

Comment [DK31]: Verwijder dit item indien beheersmaatregel A.13.2.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK32]: De media in kwestie kan worden gespecificeerd.

Comment [DK33]: De forums en sociale netwerken in kwestie kunnen worden gespecificeerd.

Comment [DK34]: Voeg toe of verwijder communicatiekanalen in overeenstemming met de risicobeoordeling en de kanalen die normaal in de organisatie worden gebruikt.

Comment [DK35]: Deze tekst kan worden vervangen door bijvoorbeeld het type gegevens en communicatiekanalen, toegestaan en verboden activiteiten voor te schrijven.

Comment [DK36]: Te verwijderen indien een dergelijk beleid niet bestaat.

Comment [DK37]: Verwijder dit item indien beheersmaatregel A.13.2.2 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

- autorisatie voor het benaderen van de informatie
- [illegible]
- [illegible]
- incidentenopvang
- [illegible]
- copyright

[illegible] opgesteld in overeenstemming met het {Beleid voor Beveiliging Leveranciers].

3.7. Systeemmonitoring

Op basis van de resultaten van de risicobeoordeling, beslist [functie] welke logs bewaard gaan [illegible]

[Functie] is verantwoordelijk voor zowel het controleren van de logs van automatisch gerapporteerde fouten op een dagelijkse basis, als ook voor het registreren van fouten [illegible] een fout, als ook hoe registraties van fouten worden bewaard]

[Functie] is verantwoordelijk voor het regelmatig bekijken van de logs om de activiteiten van de [illegible] beoordeling zal worden vastgelegd. [Functie] dient te worden geïnformeerd over de resultaten van de beoordeling

Comment [DK38]: Logs kunnen activiteiten van [illegible] gebeurtenissen, enz. bevatten.

Comment [DK39]: Verwijder dit item indien beheersmaatregel A.12.4.1 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK40]: Verwijder dit item indien beheersmaatregelen A.12.4.1 is A.12.4.3 aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK41]: Verwijder dit item indien beheersmaatregel A.12.4.1 en A.12.4.3 is aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

Comment [DK42]: Het kan worden aangegeven [illegible] voldoen aan de lokale wetgeving.

Comment [DK43]: Indien noodzakelijk, dit kan [illegible] met de bekeken systemen, hoe frequent, enz.

Comment [DK44]: Verwijder dit item indien beheersmaatregelen A.12.4.1 en A.12.4.3 zijn aangegeven als niet van toepassing in de Verklaring van Toepasselijkheid.

4. Registratiebeheer op basis van dit document

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

gebruikte communicatiekanalen] - elektronische vorm				
[Back-up proces logbestanden] – elektronische vorm	Systeem voert de back-up procedure uit	[functie]	Logbestanden zijn alleen-lezen, ze kunnen niet worden verwijderd of bewerkt	Logbestanden bewaard voor 1 jaar
[Registraties van het testen van back-up kopieën	[naam van de archiefmap/-kast]	[functie]	Alleen [functie] heeft het recht tot toegang tot degelijke registraties	Registraties worden opgeslagen voor 1 jaar
[Beveiligingsfuncties en verwachte dienstenniveau van netwerkdiensten] – elektronische en papieren vorm	[Computer van [functie]], [naam van de archiefmap/-kast]]	[functie]	Alleen [functie] heeft het recht tot toegang tot degelijke registraties	5 jaar na het vervallen van de overeenkomst van de geleverde dienst
[Verwijdering/ vernietiging registraties] - in papieren vorm	[naam van de archiefmap/-kast]	[functie]	De kast wordt afgesloten, de sleutels worden bewaard door [functies]	Registraties worden bewaard voor 5 jaar
[Registraties van logbeoordelingen] - in elektronische en papieren vorm	Computer van [functie], [naam van de archiefmap/-kast]	[functie]	Alleen [functie] heeft het recht tot toegang tot degelijke registraties	Registraties worden bewaard voor 5 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 [illegible].

Comment [DK45]: Dit is slechts een aanbeveling, pas de frequentie zo nodig aan.

Wanneer de doeltreffendheid en toereikendheid van dit document wordt beoordeeld, dan dienen de [illegible].

- aantal incidenten in verband met het veilig functioneren van de ICT systemen

- [illegible] voor het functioneren van de ICT systemen

[functie]
[naam]

_____
[handtekening]

Comment [DK46]: Alleen noodzakelijk indien de Procedure voor Beheersing voor Documenten en Registraties een ondertekening voorschrijft.