Comment [DK1]: Om te leren over het classificeren van informatie, lees dit artikel: Information classification according to ISO 27001 http://www.iso27001standard.com/blog/2014/05/12/information-classification-according-to-iso-27001/

[logo organisatie]

[naam organisatie]

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

BELEID VOOR GECLASSIFICEERDE INFORMATIE

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

Comment [DK3]: De documentcodering moet in overeenstemming zijn met het bestaande organisatie coderingssysteem; indien een dergelijk systeem niet is geïmplementeerd, dan kan deze regel worden verwijderd.

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com
in overeenstemming met de licentieovereenkomst.

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. GECLASSIFICEERDE INFORMATIE 3

3.1. STAPPEN EN VERANTWOORDELIJKHEDEN 3

3.2. CLASSIFICATIE VAN INFORMATIE 4

3.2.1. Criteria voor classificatie 4

3.2.2. Niveaus van vertrouwelijkheid 4

3.2.3. Lijst van Geautoriseerde Personen 5

3.2.4. Herclassificatie 5

3.3. LABELING VAN INFORMATIE 5

3.4. BEHANDELING VAN GECLASSIFICEERDE INFORMATIE 5

4. REGISTRATIEBEHEER OP BASIS VAN DIT DOCUMENT 8

5. GELDIGHEID EN DOCUMENTBEHEER 9

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com
in overeenstemming met de licentieovereenkomst.

1. Doel, toepassingsgebied en gebruikers

Het doel van dit document is te waarborgen dat informatie op een geschikt niveau wordt beveiligd.

Dit document is van toepassing op het hele toepassingsgebied van het Managementsysteem voor Informatiebeveiliging (ISMS), d.w.z. voor alle types van informatie, ongeacht de vorm - papieren of elektronische documenten, applicaties en databases, kennis van mensen, enz.

Gebruikers van dit document zijn alle werknemers van [naam organisatie].

2. Gerefereerde documenten

- ISO/IEC 27001 norm, clausules A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.9.4.1, A.13.2.3
- Informatiebeveiligingsbeleid
- Rapport van de Risicobeoordeling en Risicobehandeling
- Verklaring van Toepasselijkheid
- Inventarisatie van Bedrijfsmiddelen
- Lijst van Wet-, Regelgeving, Contractuele en Andere Verplichtingen
- Procedure voor Incidentbeheer
- [Procedures voor Beheersing van de Informatie en Communicatie Technologie] / [Beleid voor Verwijdering en Vernietiging]
- [Beleid voor Aanvaardbaar Gebruik]

Comment [DK4]: Indien u een dergelijke lijst niet hebt, vermeld dan alle wetgeving en contractuele verplichtingen gerelateerd aan informatiebeveiliging.

Comment [DK5]: Selecteer het document dat beveiligde gegevens voorschrijft.

3. Geclassificeerde informatie

3.1. Stappen en verantwoordelijkheden

Stappen en verantwoordelijkheden voor informatiebeheer zijn

Naam stap	*Verantwoordelijkheid*
1. [illegible]	[functie]
2. Classificatie van informatie	[illegible]
3. [illegible]	Eigenaar bedrijfsmiddel
4. Behandeling informatie	[illegible]

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com in overeenstemming met de licentieovereenkomst.

Indien de geclassificeerde informatie wordt ontvangen van buiten de organisatie, [functie] is [illegible] Beleid, en deze persoon wordt eigenaar van een dergelijk informatiebedrijfsmiddel.

3.2. Classificatie van informatie

3.2.1. Criteria voor classificatie

De classificatie (niveau van vertrouwelijkheid) wordt bepaald aan de hand van de volgende criteria:

- waarde van de informatie gebaseerd op de gevolgen beoordeeld gedurende [illegible]
- [illegible] elk item van informatie gedurende risicobeoordeling
- wetgeving en contractuele verplichtingen gebaseerd op de Lijst Wet-, Regelgeving en Contractuele Verplichtingen

3.2.2. Niveaus van vertrouwelijkheid

Alle informatie dient te worden geclassificeerd in niveaus van vertrouwelijkheid.

[illegible]	***Labeling***	[illegible]	***Toegangsbeperking***
Openbaar	[illegible]	Het openbaar maken van de [illegible]	Informatie is beschikbaar voor het publiek
[illegible]	INTERN GEBRUIK	Ongeautoriseerde toegang tot [illegible] ongemak geven	Informatie is beschikbaar [illegible] partijen
Beperkt	[illegible]	Ongeautoriseerde toegang tot [illegible] van de organisatie	Informatie is beschikbaar voor een specifieke groep [illegible] partijen
[illegible]	VERTROUWELIJK	Ongeautoriseerde toegang tot [illegible] imago van de organisatie	Informatie is alleen [illegible] individuen

Comment [DK6]: Niveau van vertrouwelijkheid en labeling kunnen worden overgenomen in het bestaande systeem in de organisatie, naar het system welke gangbaar is in de locale omgeving, of naar het system dat is voorgeschreven door wetgeving.

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com in overeenstemming met de licentieovereenkomst.

De basisregel is het laagste niveau van vertrouwelijkheid te gebruiken om een geschikt niveau van beveiliging te waarborgen, om onnodige beveiligingskosten te voorkomen.

3.2.3. Lijst van Geautoriseerde Personen

Informatie geclassificeerd als "Beperkt" en "Vertrouwelijk"dient vergezeld te gaan met een Lijst van Geautoriseerde Personen waarin de eigenaar van de informatie de namen specificeert of functies of personen die toegangsrechten hebben op die informatie.

Dezelfde regels gelden voor het niveau van vertrouwelijkheid “Intern gebruik” indien mensen buiten de organisatie toegang hebben tot een dergelijk document.

3.2.4. Herclassificatie

Eigenaren van bedrijfsmiddelen moeten het niveau van vertrouwelijkheid van hun informatiebedrijfsmiddelen elke [twee jaar] herbeoordelen en beoordelen of het niveau van vertrouwelijkheid kan worden gewijzigd. Indien mogelijk, zou het niveau van vertrouwelijkheid dienen te worden verlaagd.

Comment [D7]: Dit is slechts een aanbeveling; aan de frequentie van hebben van toegang.

3.3. Labeling van informatie

Classificatieniveaus van vertrouwelijkheid worden op de volgende manier gelabeld:

- **papieren documenten** de classificatie wordt in de rechter bovenhoek van elke pagina aangegeven, het wordt eveneens aangegeven op de voorkant van het schuifblad of enveloppe met als inhoud een dergelijk document als ook de archiefmap waarin het document wordt opgeslagen
- **elektronische documenten** de classificatie wordt aangegeven in de rechterbovenhoek van elke pagina in het document
- **informatiesystemen** de classificatie in applicaties en databases dient zowel te worden aangegeven op het inlogscherm, als ook in de rechterbovenhoek van elk daaropvolgend scherm welke de vertrouwelijke informatie laat zien
- **elektronische mail** het classificatieniveau wordt aangegeven in de eerste regel van de e-mail hoofdtekst
- **elektronische opslagmedia** (schijven, memory cards, etc.) de classificatie dient te worden aangegeven op het bovenoppervlak van een dergelijk medium
- **mondeling overgebrachte informatie** de classificatie van de vertrouwelijke informatie die van mond tot mond, telefonisch of met andere middelen wordt overgebracht dient voorafgaand aan de informatie te worden aangegeven

3.4. Behandeling van geclassificeerde informatie

Comment [D8]: Alle aangegeven regels dienen te worden aangepast aan de behoeften van de organisatie.

Alle personen die toegang hebben tot geclassificeerde (vertrouwelijke) informatie dienen de in de onderstaande label bepaalde regels te volgen. [Functie] dient disciplinaire maatregelen te inlichten telkens wanneer de regels worden overtreden of als de informatie wordt meegedeeld aan ongeautoriseerde personen. Elke gebeurtenis gerelateerd aan de behandeling van geclassificeerde

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com in overeenstemming met de licentieovereenkomst.

[illegible] met de Procedure voor Incidentbeheer.

[illegible] van de autorisatie in overeenstemming met het Beleid voor Aanvaardbaar Gebruik..

Comment [D9]: Verwijder deze paragraaf indien beheersmaatregel A.11.2.5 uitgesloten is van de Verklaring van Toepasselijkheid.

[illegible] voor Verwijdering en Vernietiging].

Comment [DK10]: Selecteer het document dat [illegible] voorschrijft.

	Intern gebruik	*Beperkt**	*Vertrouwelijk**
Papieren documenten	• alleen geautoriseerde [illegible] • [illegible] organisatie gezonden, dan dient het document te [illegible] • [illegible] gehouden zonder publieke toegang • documenten dienen [illegible] faxmachines	• het document dient te worden opgeslagen in een [illegible] • [illegible] nisatie alleen in een gesloten envelop worden [illegible] verstuurd, dan dient het document te [illegible] bevestiging • documenten dienen [illegible] • het document mag alleen worden [illegible] • [illegible] vernietigen	• het document dient te worden [illegible] • [illegible] vertrouwenswaardig persoon binnen en buiten de organisatie [illegible] envelop • het document faxen is niet toegestaan • het document mag [illegible] printer staat
[illegible]	• alleen geautoriseerde [illegible] hebben	• alleen personen met een autorisatie voor dit document	• het document dient [illegible]

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com in overeenstemming met de licentieovereenkomst.

	• wanneer bestanden [illegible] beveiligd met een wachtwoord • toegang tot de informatie [illegible] sterk wachtwoord • het scherm waarop het [illegible] te gaan na [aantal] minuten van inactiviteit	mogen toegang hebben tot het deel [illegible] is opgeslagen • wanneer bestanden worden [illegible] enz., dan dienen ze te worden versleuteld • alleen de [illegible] verwijderen	versleutelde vorm • het document mag [illegible] beheerst door de organisatie • het document dient niet te worden [illegible] enz.
Informatie [illegible]	• alleen geautoriseerde [illegible] hebben • toegang tot informatie- [illegible] wachtwoord • het scherm waarop het [illegible] minuten van inactiviteit • het informatiesysteem mag alleen in ruimten worden geplaatst met fysieke toegangs-beveiliging	• gebruikers dienen uit het [illegible] de werkplek hebben verlaten • gegevens moeten [illegible] vernietiging garandeert	• toegang tot het informatiesysteem [illegible] van smart cards of biometrische lezers • het informatie-systeem mag alleen [illegible] • het informatie-systeem mag alleen [illegible] ruimte betreden
[illegible] **mail**	• alleen geautoriseerde [illegible]	• e-mail dient te worden versleuteld	• [illegible] worden versleuteld

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com
in overeenstemming met de licentieovereenkomst.

	hebben • de verzender dient [illegible] • [illegible] "Informatiesystemen" gelden	indien deze naar [illegible] verzonden	
Elektronische [illegible] media	• alleen geautoriseerde personen mogen toegang [illegible] • [illegible] moeten dienen te worden beveiligd met een [illegible] • [illegible] worden verstuurd als geregistreerde post • het medium mag alleen in [illegible] beveiliging	• media en bestanden [illegible] • [illegible] worden opgeslagen in een afgesloten kast • indien verzonden [illegible] met een ontvangst-bevestiging • alleen de eigenaar [illegible] vernietigen	• media dienen te [illegible] • [illegible] persoon binnen en buiten de organisatie worden overgebracht [illegible] envelop
Mondelinge overgebrachte informatie	• alleen geautoriseerde personen mogen toegang [illegible] • [illegible] informatie wordt gecommuniceerd	• de ruimte moet [illegible] • [illegible] opgenomen	• conversatie gehouden door een [illegible] versleuteld • geen transcriptie van [illegible]

*Maatregelen worden cumulatief geïmplementeerd, wat betekent dat maatregelen voor elk [illegible] dan dienen alleen degelijke maatregelen te worden geïmplementeerd

4. Registratiebeheer op basis van dit document

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com
in overeenstemming met de licentieovereenkomst.

Naam registratie	Opslaglocatie	Persoon verantwoordelijk voor opslag	Beveiligingsmaatregelen voor registraties	Bewaartermijn
[Lijs van Geautoriseerde Personen met toegang tot documenten]	Tezamen met de informatie waar het classificatie-niveau is aangegeven	Eigenaar informatie-bedrijfsmiddel	Hetzelfde voor de beveiliging van informatie	De lijst dient te bestaan net zolang als de informatie zelf bestaat

5. Geldigheid en documentbeheer

Dit document is geldig vanaf [datum].

De eigenaar van dit document is [functie]. Hij/zij dient het [illegible] één keer 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 [illegible]

- [illegible]
- aantal van informatiebedrijfsmiddelen die met een ongepast classificatieniveau zijn geclassificeerd

[functie]
[naam]

_____
[handtekening]

Comment [DK12]: Alleen noodzakelijk indien de Procedure voor Beheersing van Documenten en Registraties voorschrijft dat papieren documenten dienen te worden ondertekend.

©2015 Deze sjabloon mag worden gebruikt door klanten van EPPS services Ltd. www.iso27001standard.com
in overeenstemming met de licentieovereenkomst.