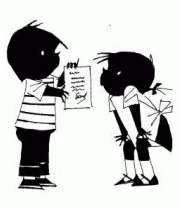
NEN

NEN 7510 | Informatiebeveiliging in de zorg



Introductie

Wie ben ik en wat doe ik?

Wim Jellema

Staffunctionaris Privacy & Informatieveiligheid

DIMENCE GROEP

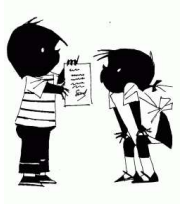
Bovenstaande is mijn ‘formele’ functietitel. In de praktijk geef ik invulling aan de CISO rol en de rol van Privacy Officer en leg ik verantwoording af aan de RvB.

De DG kent een security team, bestaande uit de CISO, 2 technische ISO’s en een systeembeheerder security.

Dit team geeft invulling aan de security vraagstukken die spelen. De FG sluit periodiek aan in het teamoverleg.

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Introductie

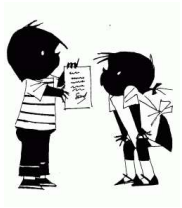
Spannend zo’n korte film, vast een Netflix productie ☺!

Al met al……..

is cybersecurity en daarmee dus ook informatiebeveiliging toch wel een dingetje en moeten we ons bewust zijn van de risico’s en voldoende aandacht hebben voor zowel de techniek als de fysieke en digitale data en niet te vergeten de mens!

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Introductie

Definitie van informatiebeveiliging?

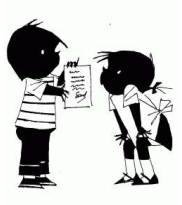
Er zijn natuurlijk meerdere definities, maar volgens Wikipedia (het woord is namelijk nog niet opgenomen in de Van Dale):

“Informatiebeveiliging is het geheel van preventieve , detectieve, repressieve en correctieve maatregelen alsmede procedures en processen die de beschikbaarheid, exclusiviteit en integriteit van alle vormen van informatie binnen een organisatie of een maatschappij garanderen, met als doel de continuïteit van de informatie en de informatievoorziening te waarborgen en de eventuele gevolgen van beveiligingsincidenten tot een acceptabel, vooraf bepaald niveau te beperken.”

Duidelijk toch? Of toch niet?

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

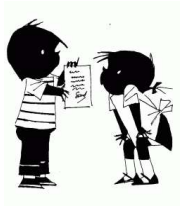
Introductie

Beter is dat we het opsplitsen

- Onder ‘informatie’ verstaan we (onder andere) persoonsgegevens, intellectueel eigendom, bedrijfsgevoelige informatie, of informatie van je cliënten, patiënten, medewerkers en relaties.
- Met (informatie)beveiliging wil je als organisatie ongewenste toegang tót en de verwerking en vernietiging ván informatie voorkomen.
- Daarnaast wil je ook de gevolgen van een mogelijk datalek minimaliseren.
- Dit alles is dan een combinatie van beleid, procedures en maatregelen.

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Introductie

Waarom informatiebeveiliging?

Omdat je de informatie, waarvan je hebt vastgesteld dat deze belangrijke waarde vertegenwoordigt voor de organisatie, wil beschermen.

Omdat cybercriminaliteit overhand toeneemt met ernstige gevolgen. Denk aan diefstal van persoons- of bedrijfsgegevens, uitval van ICT diensten en afpersingen.

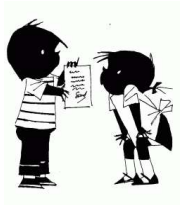
Omdat er steeds meer wet- en regelgeving op het gebied van informatiebeveiliging komt.

Omdat (potentiële) klanten steeds strengere eisen stellen aan- en/of hoge verwachtingen hebben van- de omgang met hun gegevens.

…….. dus moeten we informatiebeveiliging serieus nemen.

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

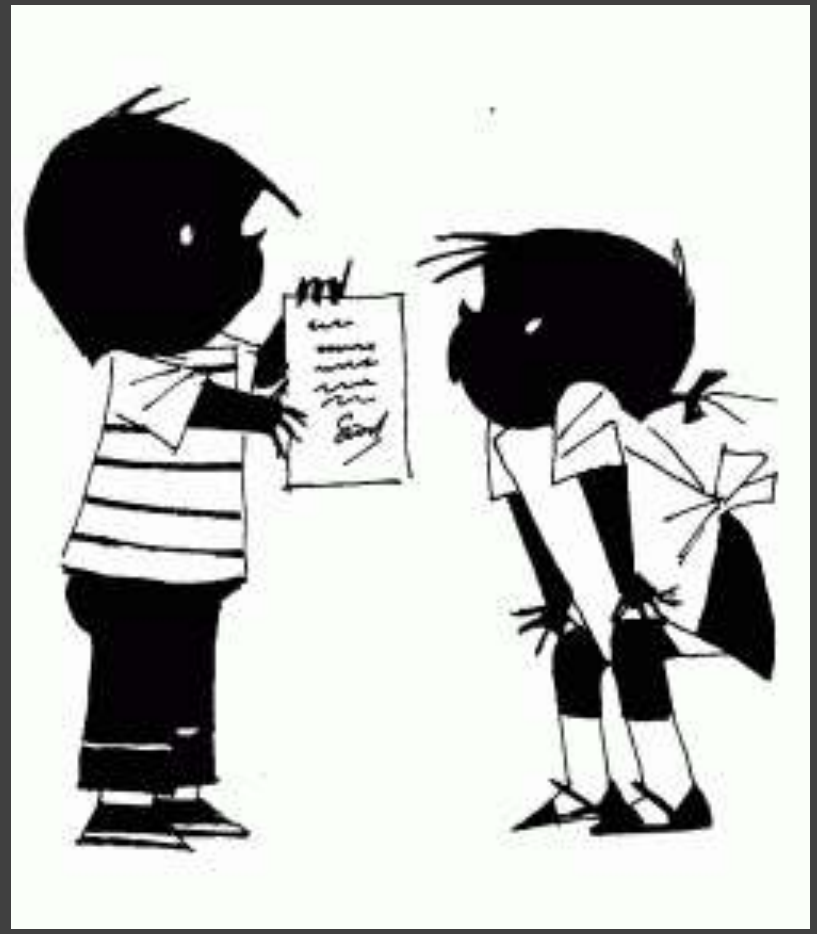
Introductie

Én dus,

moet je informatiebeveiliging in de organisatie integreren én komt een norm als ISO 27001 of NEN 7510 om de hoek kijken, waarin omschreven staat hoe je informatiebeveiliging procesmatig kan inrichten.

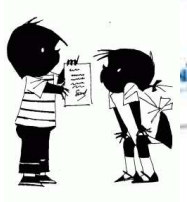
NEN

NEN 7510 | Informatiebeveiliging in de zorg



NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

NEN 7510

NEN 7510 is een **Ne**derlandse **N**orm voor informatiebeveiliging in de zorg, gebaseerd op de internationale norm ISO 27001 en deze bestaat tegenwoordig, net als de ISO norm, uit **2** delen. Beide delen zijn *gratis* te downloaden op de site van de NEN.

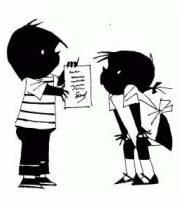
De norm beschrijft welke maatregelen genomen moeten worden om op de juiste manier om te kunnen gaan met patiëntgegevens en zorgt dat de processen rondom informatiebeveiliging gecontroleerd verlopen.

NEN 7510 op een rij:

- Norm ontwikkelt door het Nederlands Normalisatie Instituut.
- Norm gericht op informatiebeveiliging in de zorg.
- Voortgekomen uit ‘Code voor informatiebeveiliging’ (tegenwoordig ISO 27001/27002)
- Nederlandse norm, niet bekend in het buitenland
- Zorg specifieke invulling van de ISO 27001

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

NEN 7510

Waarom een aangepaste versie voor de zorg?

Binnen de zorg ligt de focus meer op patiëntgegevens met vervolgens uiteraard extra specifieke aandachtspunten zoals bijvoorbeeld privacybescherming. Zo zijn de beheersmaatregelen zoals ze voorkomen in de ISO 27002 in de NEN 7510 aangevuld met één of meerdere zorgspecifieke maatregelen en is ook de zorgspecifieke implementatierichtlijn aangegeven.

Uiteraard is het mogelijk dat niet alle implementatie-richtlijnen geheel passend zijn gelet op de gestelde eisen m.b.t. de beheersmaatregelen van de organisatie.

Informatiebeveiliging

NEN 7510

Voorbeeld

Zorgspecifieke implementatierichtlijn

NEN 7510 | Informatiebeveiliging in de zorg

A.12.3 Back-up		
Doelstelling: Beschermen tegen het verlies van gegevens.		
A.12.3.1	**Back-up van informatie**	***Beheersmaatregel*** Regelmatig moeten back-upkopieën van informatie, software en systeemafbeeldingen worden gemaakt en getest in overeenstemming met een overeengekomen back-upbeleid. **ZORGSPECIFIEKE BEHEERSMAATREGEL** Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is. Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Informatiebeveiliging

NEN 7510; 2 delen

Deel 1 Managementsysteem

(hier kun je op certificeren, niet op deel 2!)

Deel 1 vereist dat je inzicht krijgt in de organisatie, wat de behoeften en verwachtingen zijn en op basis van het beoordelen van risico's kom je tot eisen voor het vaststellen , implementeren, uitvoeren, controleren, beoordelen en continu verbeteren van informatiebeveiliging.

Dit deel beschrijft dus dat je een ISMS, afkorting voor Information Security Management Systeem, moet inrichten ofwel een Plan Do Check Act cirkel om het niveau van informatiebeveiliging continue te verbeteren.

Het managementsysteem voor informatiebeveiliging (ISMS) omvat structuur, beleid, planningsactiviteiten, verantwoordelijkheden, werkwijzen, procedures, processen en middelen van de organisatie.

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Informatiebeveiliging

NEN 7510; 2 delen

Deel 1 Managementsysteem

in andere woorden;

Een ISMS is dus geen tool, maar een proces

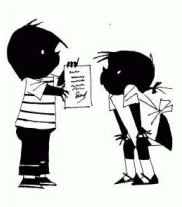
Met een Information Security Management System wordt niet gedoeld op een systeem in de vorm van een softwaretool, maar op een continu verbeterproces. Een ISMS is dan ook geen op zichzelf staand systeem, maar juist een **manier van werken**. Een manier van werken waarbij een systematische aanpak wordt gehanteerd om (vertrouwelijke) informatie te managen, zodat de veiligheid ervan wordt gewaarborgd.

Een ISMS kan naar eigen inzicht ingericht en bestuurd worden. Dat neemt echter niet weg dat er wel degelijk een aantal specifieke eisen worden gesteld waaraan een ISMS dient te voldoen. Vanuit de norm wordt namelijk gevraagd om een managementsysteem in te richten, te implementeren, te onderhouden en continu te verbeteren. Dat laatste kan bijvoorbeeld met behulp van de Plan-Do-Check-Act (PDCA) verbetercyclus.

Een vast onderdeel van die verbetercyclus, en in feite de basis van je ISMS, is de uitvoering van risicoanalyses. Daarmee worden specifieke interne en externe organisatierisico's rondom informatiebeveiliging in kaart gebracht en vervolgens verlaagd door passende beveiligingsmaatregelen.

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

NEN 7510; 2 delen

Deel 2 Maatregelen

Deel 2 bestaat uit 18 hoofdstukken, waarbij hoofdstuk 5 t/m 18 elk een doelstelling bevat, die aangeeft wat bereikt moet worden en die de verschillende beheersmaatregelen aangeeft die moeten worden toegepast om de doelstelling te behalen.

- 0 Inleiding
- 1 Onderwerp en toepassingsgebied
- 2 Normatieve verwijzingen
- 3 Termen en definities
- 4 Structuur van de paragrafen
- 5 Informatiebeveiligingsbeleid
- 6 Organiseren van informatiebeveiliging
- 7 Veilig personeel
- 8 Beheer van bedrijfsmiddelen
- 9 Toegangsbeveiliging
- 10 Cryptografie
- 11 Fysieke beveiliging en beveiliging van de omgeving
- 12 Beveiliging bedrijfsvoering
- 13 Communicatiebeveiliging
- 14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen
- 15 Leveranciersrelaties
- 16 Beheer van informatiebeveiligingsincidenten
- 17 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer
- 18 Naleving

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Informatiebeveiliging

NEN 7510

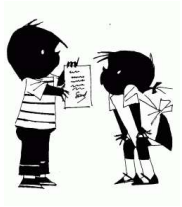
Wat nu te doen?

Pak de norm en neem deze eens rustig door. Je ziet dat, zoals eerder al aangegeven, de NEN 7510-1 en NEN 7510-2 richtlijnen en uitgangspunten geven voor het bepalen, instellen en handhaven van maatregelen die je als zorginstelling van persoonlijke gezondheidsinformatie moet treffen ter beveiliging van de informatievoorziening.

De norm geeft hiervoor een raamwerk in de vorm van een managementsysteem voor informatiebeveiliging (ISMS).

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

NEN 7510

Wat nu te doen?

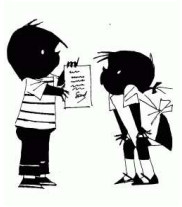
Je hoeft niet zelf het wiel te gaan uitvinden voor het opzetten van een managementsysteem voor informatie-beveiliging conform de NEN 7510. Er zijn vele deskundig adviseurs die jou en jouw organisatie kunnen ondersteunen om de stappen te doorlopen om te voldoen aan de NEN 7510.

Ook zijn er diverse ondersteunende ISMS software oplossingen te verkrijgen die het gehele proces en de invulling van maatregelen inzichtelijk maken en ondersteunen.

Je kunt natuurlijk echter ook eerst zelf een start maken!

NEN

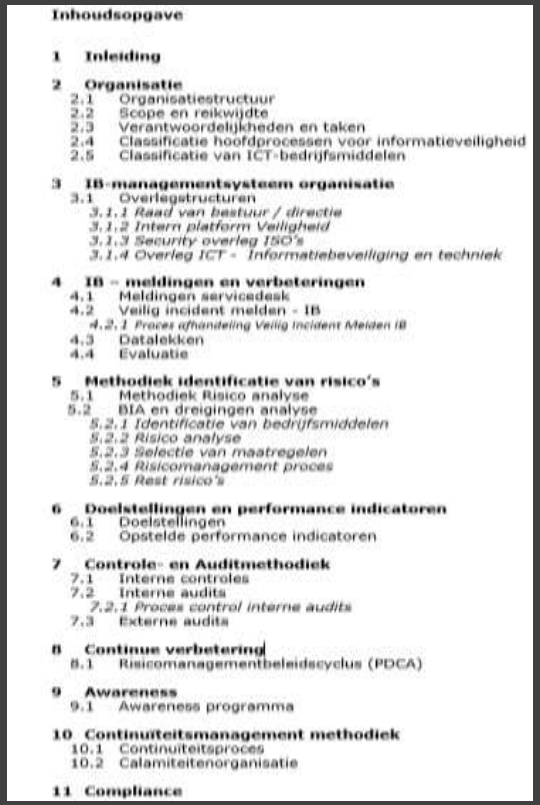
NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Starten in Word & Excel

Realiseer bijvoorbeeld een ‘uitwerking’ / ‘handboek informatiebeveiliging’ waarin je weergeeft hoe de informatiebeveiliging in je organisatie is ingeregeld of gaat worden ingeregeld (de werkwijze en activiteiten m.b.t. informatiebeveiliging).

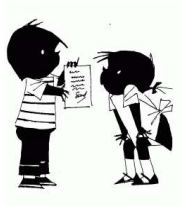


Inhoudsopgave

En zie daar je ISMS heeft vorm gekregen!

NEN

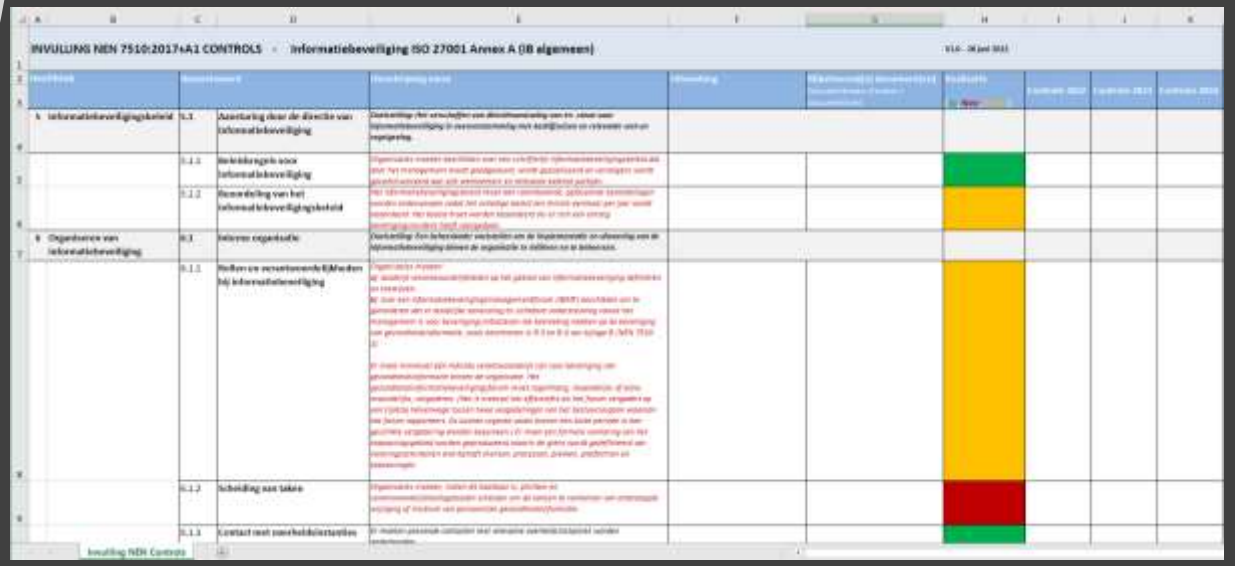
NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Starten in Word & Excel

Neem vervolgens alle normelementen op (met of zonder omschrijving), noteer je uitwerking, noteer de bijbehorende documenten (naam, locatie of documentlink), via een kleurtje geef je aan of je al volledig voldoet aan het betreffende normelement en wanneer een controle plaats heeft.

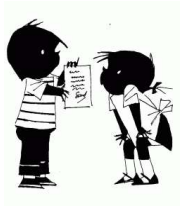


Met beperkte aanpassing kan een document als deze ook dienst gaan doen als verklaring van toepasselijkheid*!

*** Een opsomming van maatregelen van toepassing voor een organisatie , die geïmplementeerd dienen te worden om risico's te mitigeren.**

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

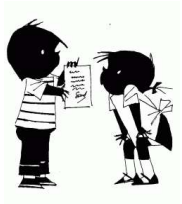
Starten in Word & Excel

Zorg voor de volgende verplichte documentatie/documenten, vanuit de NEN 7510 deel 1 en 2.

	NEN 7510:2017 delen I + II
Gedocumenteerde informatie	Onderdeel
- Scope van het ISMS	I - 4.3
- Informatiebeveiligingsbeleid en doelen	I - 5.2, 6.2
- Risico analyse, - behandeling en -methode	I - 6.1.2
- Verklaring van toepasselijkheid	I - 6.1.3 d
- Risicobehandelplan	I - 6.1.3e, 6.2
- Procedure gedocumenteerde informatie	I - 7.5.3
- Definitie van taken, verantwoordelijkheden en bevoegdheden tav informatiebeveiliging	II - 7.1.2, II - 13.2.4
- Eisen mbt vertrouwelijkheid en non-disclosure agreements	II - 7.1.2
- Gebruik van bedrijfsmiddelen	II - 8.1.1
- Aanvaardbaar gebruik van bedrijfsmiddelen	II - 8.1.3
- Logisch toegangsbeleid	II - 9.1.1
- Fysieke beveiliging: zones, procedures beveiligde ruimten	II - 11.1
- Operationele procedures voor IT management	II - 12.1.1
- Procedure back-up and restore	II - 12.3.1
- Principes voor engineering	II - 14.2.5
- Beleid informatiebeveiliging toeleveranciers	II - 15.1.1
- Incident management procedure	II - 16.1.5
- Business continuity procedures	II - 17.1.2
- Eisen mbt wet- en regelgeving	II - 18.1.1
- Registraties van trainingen, skills, ervaring en kwalificaties	I - 7.2
- Monitoring and meetresultaten	I - 9.1
- Internal audit programma	I - 9.2
- Resultaten van internal audits	I - 9.2
- Resultaten van management review	I - 9.3
- Resultaten van correctieve acties	I - 10.1
- Contractvoorwaarden medewerkers mbt informatiebeveiliging, disciplinaire maatregelen	II - 7.1.2
- Logging van gebruikers activiteiten, uitzonderingen en security events	II - 12.4.1, II - 12.4.3

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Starten in Word & Excel

Voorbeeldplanning

	Planning Informatieveiligheid (NEN 7510) 2022
	Plan fase
Actie	Algemeen
1	***Opstellen Plan van Aanpak Informatieveiligheid (PVA)***
2	Vaststellen PVA
3	Communicatie PVA richting Directies en management
4	(Hoofd)processen definieren t.b.v. informatiebeveiliging (IB) en vaststellen
5	Realiseren van een handboek informatiebeveiliging (beschrijvende versie ISMS)
	beschrijving:
	- organisatiestructuur, scope, processen, rollen en verantwoordelijkheden
	- overlegstructuren
	- doelstellingen
	- methodiek van risiscoanalyse, risicobehandeling
	- continuïteitsmanagement
	- awareness
	- incidentmeldingen
	- continue verbeteren (PDCA)
	Do fase
6	Uitvoeren Risicoanalyse (bv. BIA en DA) op hoofdprocessen en belangrijke ICT middelen
	- verwerking uitkomst Risico Analyse
7	Opstellen van de Verklaring van Toepasselijkheid (VVT) (gekozen beheersdoelstellingen en maatregelen met onderbouwing)
	Awareness
8	Kerngroep informatiebeveiliging instellen
9	Uitvoering acties - vergroten awareness bij medewerkers - door Kerngroep
	- Intranetdocument(en), Posteractie, Login melding, e-learning
	- Introductietraining nieuwe medewerkers
	- Voorlichtingsessies
	- Opstellen terugkerend jaarprogramma
	Communicatie
10	Communicatie richting OR
11	Communicatie richting RvB/Directie en Management
12	Communicatie richting medewerkers
13	doorlopende communicatie tbv uitrol en voortgang (management, medewerkers)

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Informatiebeveiliging

Starten in Word & Excel

Voorbeeldplanning - vervolg

	Implementatie ISMS
14	Resterende acties n.a.v. punt 5
15	Doorvoeren maatregelen n.a.v. VVT
	- opstellen procedures
	- opstellen gedragscodes
	- inregelen technische maatregelen
	- inregelen fysieke maatregelen
16	Op te leveren basis documenten
	Handboek informatiebeveiliging (beschrijvende versie ISMS)
	Informatiebeveiligingsbeleid
	Verklaring van toepasselijkheid
	Informatiebeveiligingsplan
	Classisficatiesystematiek informatiesystemen
	Opzet baseline beveiliging (wat minimaal moet voor ieder ICT-middel of IS)
	Continuiteitsplan
	Check fase
	Monitoren en beoordelen
17	Check op effectiviteit maatregelen
18	Check op reducering risico's
19	Controle behalen doelstelling
20	Uitvoeren 'Interne Audit' (verplicht voor certificering NEN 7510)
	Act fase
	Verbeteren
21	Uitvoering van acties voortkomend uit de Check fase
	- herschrijven procedures
	- treffen van corrigerende maatregelen
	- treffen van preventieve maatregelen
	- bevindingen interne audit oplossen
22	Aandacht voor de verbeterpunten ISMS

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Informatiebeveiliging

Starten in word & Excel

Tip1

In de norm staat nergens dat je voor elke beheersmaatregel een apart document moet schrijven. Ook staat nergens dat je beleidsdocumentatie in een bepaalde vorm moet kunnen presenteren.

Tip2

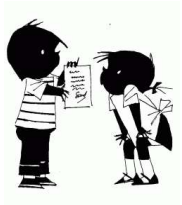
Beleid heeft een bepaalde houdbaarheidsdatum. Het kan zijn dat naar aanleiding van een incident of verandering van de omgeving het gevoerde beleid niet meer blijkt te voldoen en dus bij deze constatering je beleid aanpassen. Beter is de beoordeling van het beleid en (verplichte) documenten op te nemen als periodieke controle actie.

Tip3

Het internet biedt veel informatie, templates en voorbeeld documenten. Ook collega instellingen kunnen mogelijk helpen!

NEN

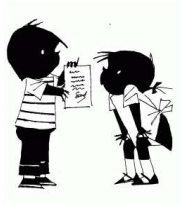
NEN 7510 | Informatiebeveiliging in de zorg



Dank voor de aandacht en succes met de implementatie NEN7510

NEN

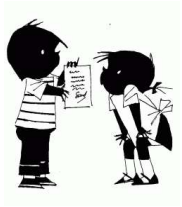
NEN 7510 | Informatiebeveiliging in de zorg



Dank voor de aandacht en succes met de implementatie NEN7510

NEN

NEN 7510 | Informatiebeveiliging in de zorg



Informatiebeveiliging

Toegift

Medewerkers bewust maken, een heel belangrijk onderdeel van informatie beveiliging!

Niet zomaar gegevens delen……


Welkom in de wondere
wereld van Dave

NEN

NEN 7510 | Informatiebeveiliging in de zorg

Einde