KWINZO

Eugenie Verhaar

Kwinzo vanaf 2017, inrichten ISMS → ISO 27001 /NEN 7510

Gestandaardiseerde aanpak, templates, applicatie

Hoe het begon

- Dit is het verhaal van Fenelab Consortium Covid-19 (nu 1st LAB consortium), dat in juni 2021 meedeed aan een aanbesteding van VWS voor ‘testen voor toegang’.
- Een van de eisen: Voldoe aantoonbaar aan de NEN 7510
- 1st LAB consortium is de uitdaging aangegaan, ze zijn nu gecertificeerd

Is hier sprake van het begin van een trend? Wordt deze eis standaard?

KWINZO

Trend? Standaard eis?

- Wat gaat de NVWA doen?
- Wordt de ISO 27001 standaard meegenomen als eis bij aanbestedingen?
- Voor medische labs: beveiliging persoonsgegevens cruciaal
- Behandelrelatie → NEN 7510

KWINZO

Inhoud

- Wat is informatiebeveiliging?
- Waarom wil ik dat?
- Wat moet ik dan doen?

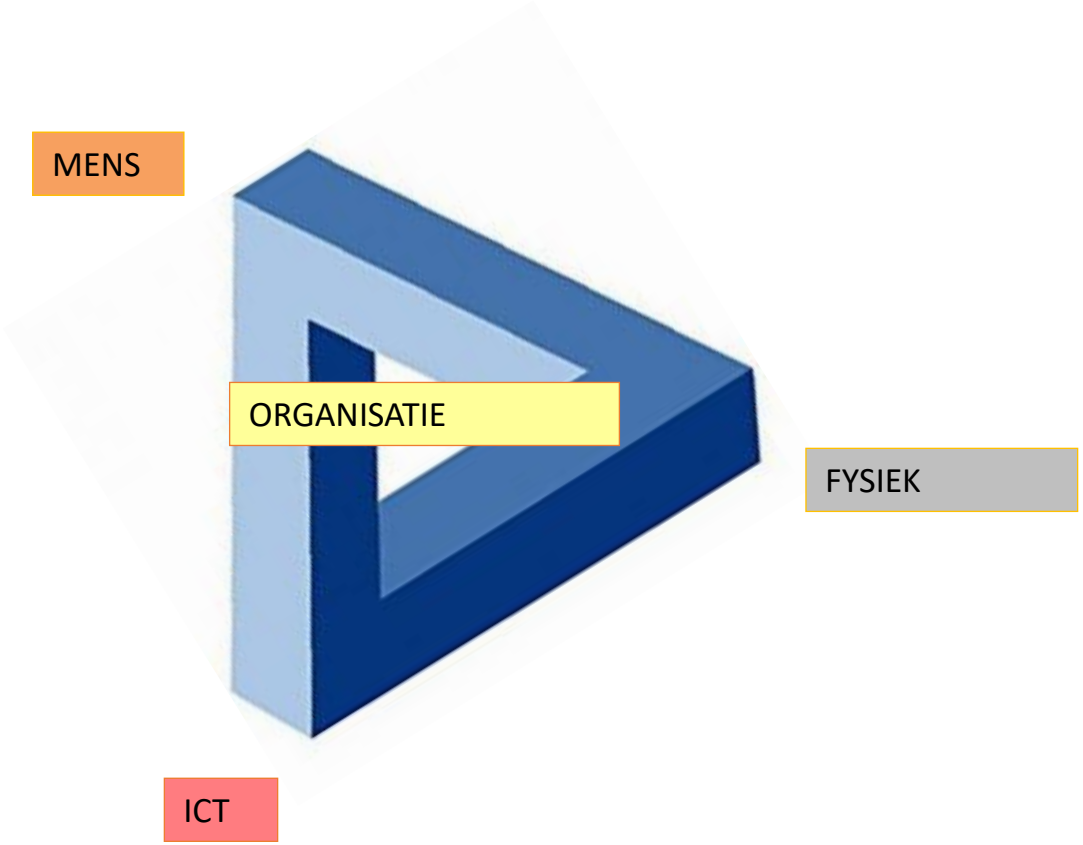
KWINZO

Wat is informatiebeveiliging?

- Beschikbaarheid
- Integriteit (correctheid)
- Vertrouwelijkheid

KWINZO

Vier soorten maatregelen



NEN 7510 en ISO 27001

- NEN 7510 = de ISO 27001 voor de zorg.
- De ISO 27001 is **het** normenkader voor informatiebeveiliging.

De NEN 7510 = ISO 27001 aangevuld met eisen tav omgang met patiëntgegevens.

KWINZO

Waarom wil ik dat?

Immers: ISO 17025 en ISO 15189 vragen ook om Plan Do Check Act met:

- Governance.
- Beleid, doelstellingen, uitgangspunten.
- Risicomanagement.
- Overzichten met bedrijfsmiddelen.
- Periodieke controles en rapportages .
- Etc etc

KWINZO

En ook specifiek informatiebeveiliging:

- NEN 17025: 7.11 Control of data and information management
- NEN 15189: 5.10: Laboratoriuminformatiemanagement

Wat voegen de NEN 7510 /ISO 27001 dan toe?

KWINZO

NEN 7510 /ISO 27001

+

De Annex met

Beheersmaatregelen, op

alle beveiligingsterreinen

KWINZO

Annex: 14 hoofdstukken

6 hoofdstukken gericht op ICT – technische maatregelen:

- Encryptie
- Autorisaties, wachtwoordbeheer, authenticatie
- Netwerken
- Software ontwikkeling
- Managen ICT-leveranciers
- Continuïteit van ICT voorzieningen

Voorbeelden

A.10 Cryptografie		
A.10.1 Cryptografische beheersmaatregelen		
Doelstelling: Zorgen voor correct en doeltreffend gebruik van cryptografie om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen.		
A.10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	*Beheersmaatregel* Ter bescherming van informa voor het gebruik van cryptogr beheersmaatregelen worden geïmplementeerd.
A.10.1.2	Sleutelbeheer	*Beheersmaatregel* Met betrekking tot het gebrui de levensduur van cryptograf tijdens hun gehele levenscyclu ontwikkeld en geïmplemente
A.11 Fysieke beveiliging en beveiliging van de omgeving		

A.12.2 Bescherming tegen malware		
Doelstelling: Waarborgen dat informatie en informatieverwerkende faciliteiten beschermd zijn tegen malware.		
A.12.2.1	Beheersmaatregelen tegen malware	*Beheersmaatregel* Ter bescherming tegen malware moeten beheersmaatregelen voor detectie, preventie en herstel worden geïmplementeerd, in combinatie met een passend bewustzijn van gebruikers.
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.

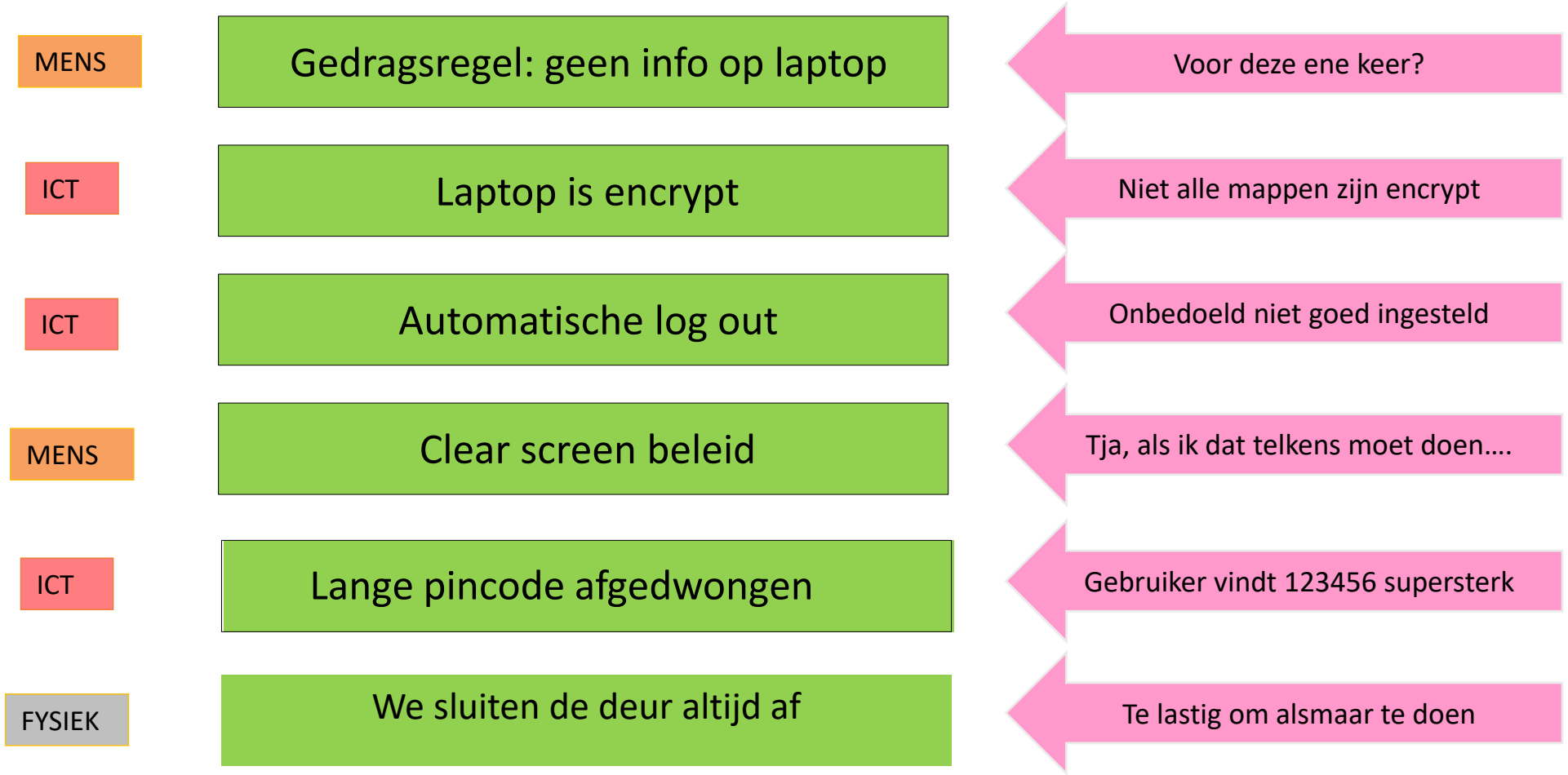
KWINZO

Terug naar Fenelab, wat heeft het gebracht?

- Compleet overzicht van alle data, applicaties, hardware, meetinstrumenten
- Inzicht in bedreigingen en risico’s
- Samenhangend stelsel van beveiligingsmaatregelen
- Controles en aantoonbaarheid.

KWINZO

Beveiliging informatie op een laptop



Belangrijke bedreigingen /risico’s

- Onbeveiligde Mobile devices
- Slechte omgang met opslagmedia (USB- sticks, harde schijven)
- Onvoldoende beveiliging meetinstrumenten
- Ransomware
- Onbetrouwbare (ex) medewerkers en externen
- Onvoldoende toezicht op autorisaties
- Onvoldoende toezicht op leveranciers met toegang tot data ICT
- Diefstal (humaan) materiaal en laboratoriumuitslagen

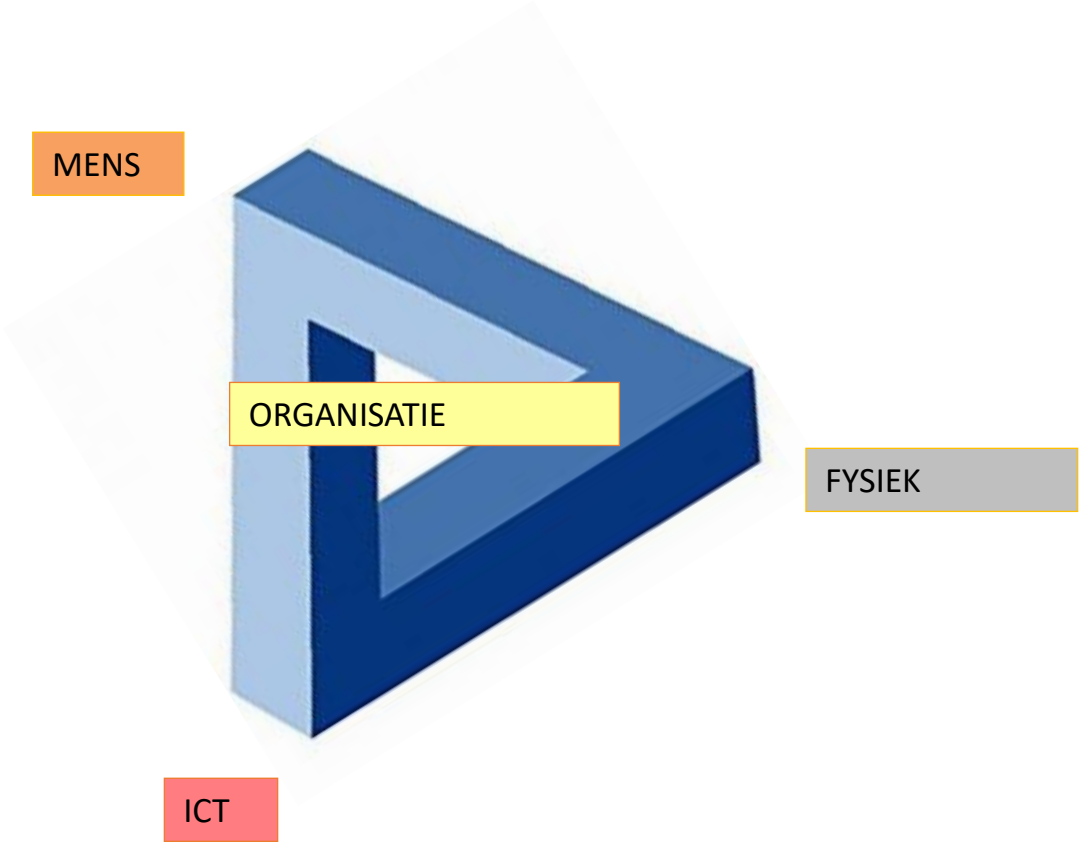
KWINZO

Belangrijke beveiligingsmaatregelen

- Beveiliging (encryptie) Mobile devices,
- Maatregelen tegen ransomware (firewalls, back ups, Restore oefening)
- Verscherpte controles op autorisaties (ook van beheerders)
- Calamiteitenplan uitgebreid met reactie op ‘informatierampen’
- Sluitend Leveranciersmanagement, overeenkomsten, audits,
- Periodieke penetratietesten op applicaties
- Gedrag en bewustwording medewerkers

KWINZO

In samenhang met elkaar



Kortom

Informatie wordt steeds belangrijker

De ‘lab normen’, gaan hier niet diep op in

Je hebt zo geen zekerheid dat de informatievoorziening echt op orde is

En dat je voldoet aan wetgeving op dit terrein.


Bijna alles is informatie!