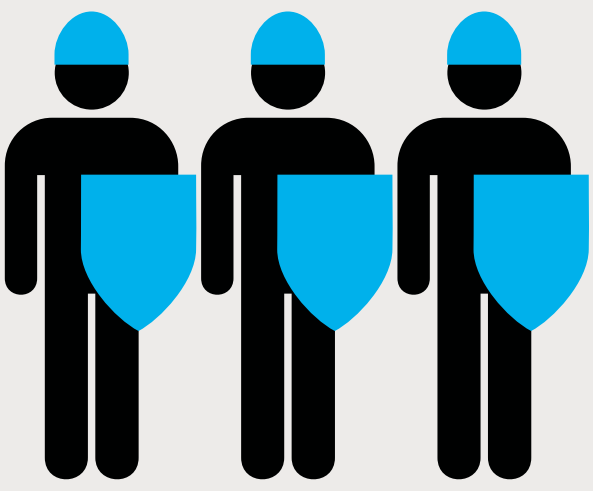
INFORMATIEBEVEILIGING

7 praktische tips

Met deze zeven praktische tips kunt u als zorginstelling of praktijk uw informatiebeveiliging verbeteren. Sommige tips lijken voor de hand liggend. De praktijk wijst echter uit dat de informatiebeveiliging juist op deze praktische punten nog wel eens beter kan. Dit blijkt uit een inventarisatie over informatiebeveiliging bij 40 apotheken en 36 huisartsenpraktijken. We hebben onze bevindingen in deze tips 'versleuteld'.

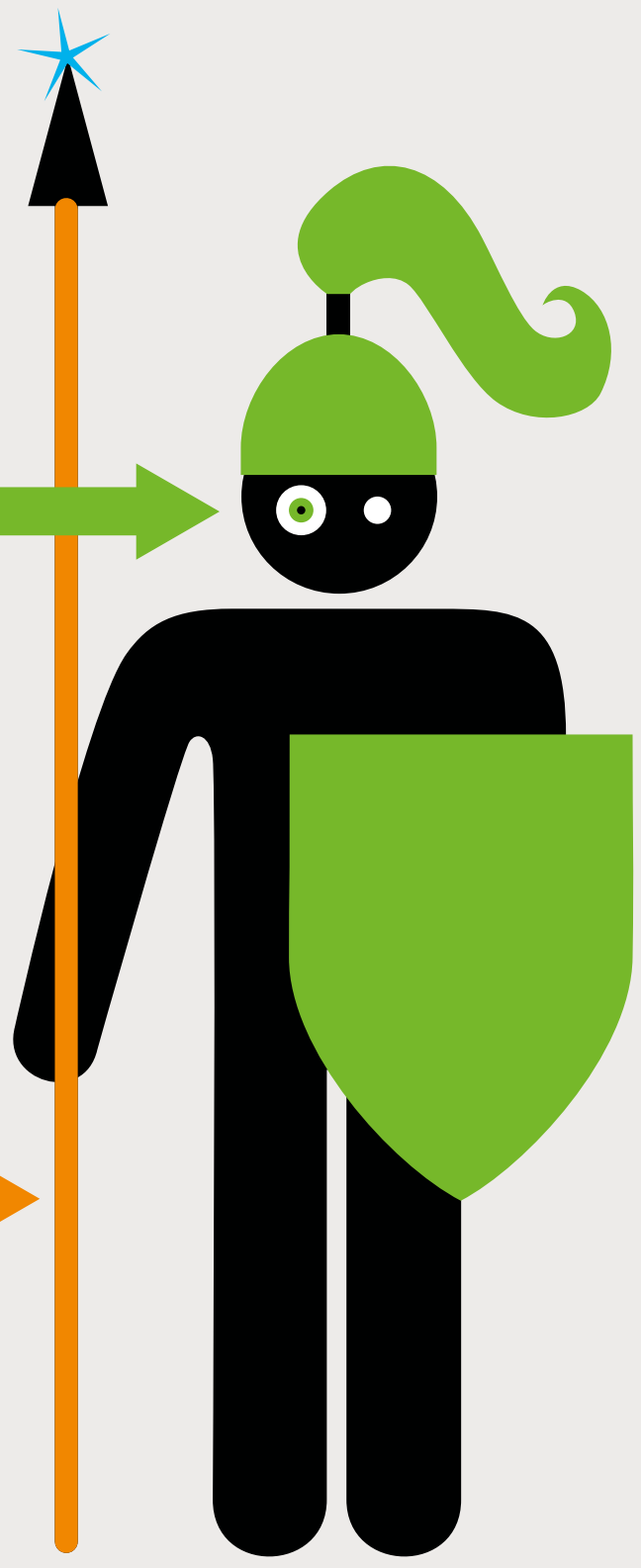


1. STIMULEER BEVEILIGINGS-BEWUSTZIJN BIJ MEDEWERKERS

- Geef het goede voorbeeld aan collega's door zelf beveiligingsbewust te werken.
- Zorg voor duidelijke en werkbare instructies voor het veilig werken met digitale informatie.
- Creëer een werksfeer waarbij medewerkers elkaar stimuleren veilig om te gaan met patiëntgevoelige informatie en elkaar indien nodig kunnen aanspreken.

2. CONTROLEER REGELMATIG OP VERDACHTE INZAGE IN PATIËNTENGEGEVENS

- Controleer regelmatig (bij voorkeur dagelijks, maar minimaal wekelijks) de logbestanden op verdachte inzage in patiëntgegevens.
- Informeer uw omgeving dat u de logbestanden controleert.
- Raadpleeg uw ICT-leverancier indien niet duidelijk is hoe u de logbestanden kunt bekijken.



3. BESCHERM PC'S TEGEN COMPUTERVIRUSSEN

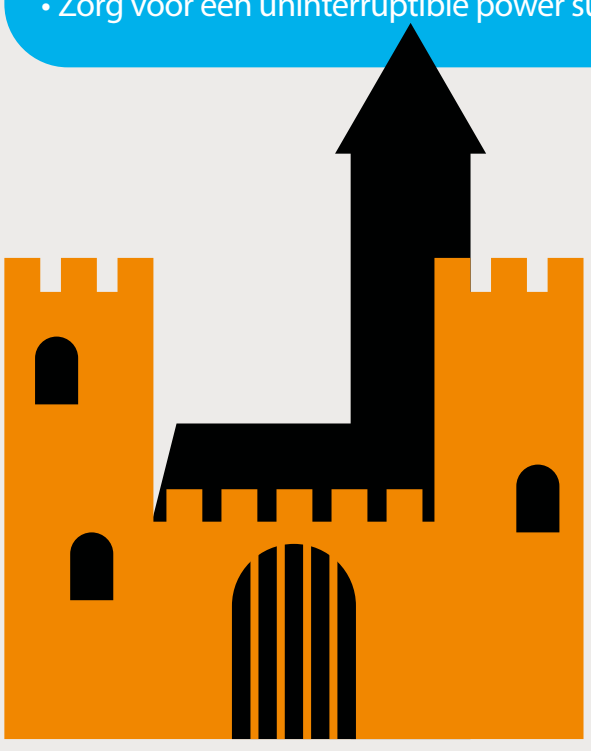
- Zorg dat iedere pc is voorzien van een actuele virusscanner.
- Zorg dat de virusscanner up-to-date is.
- Wees voorzichtig met het openen van bijlagen in e-mails.
- Installeer geen programma's van onbekende herkomst.

4. VOORKOM PROBLEMEN MET ICT-CONTRACTEN

- Zorg voor een up-to-date contract met de ICT-leverancier.
- Wees ervan bewust welke afspraken via het contract zijn gemaakt.

5. BESCHERM DE SERVER TEGEN BESCHADIGING, UITVAL EN DIEFSTAL

- Beveilig uw pand tegen inbraak, onderzoek of er inbraakgevoelige plaatsen zijn.
- Zet de server niet op de grond bij een werkplek, maar in een aparte serverruimte.
- Zet de server niet op de grond en niet op een plek met risico op waterschade.
- Zorg dat onbevoegden niet in de serverruimte kunnen.
- Zorg voor voldoende koeling in de serverruimte.
- Zorg voor een uninterruptible power supply (UPS).



6. MAAK REGELMATIG EEN BACK-UP EN BEWAAR DEZE OP EEN VEILIGE LOCATIE

- Maak dagelijks een back-up.
- Bewaar de back-up op een veilige plaats, bijvoorbeeld buiten het pand.
- Zorg dat de back-up door een vervanger wordt gemaakt tijdens afwezigheid van de vaste persoon die de back-up maakt.
- Ga zorgvuldig om met de back-up, er staan patiëntgegevens op.

7. VERNIETIG AFGEDANKTE OPSLAGMEDIA

- Vernietig de digitale opslagmedia zorgvuldig.
- Vraag advies aan uw ICT-leverancier of aan een datavernietigingsbedrijf.

OVER DEZE INFOGRAPHIC Deze infographic kan een bijdrage leveren aan de beveiliging van informatie in uw organisatie. Het gaat over de praktische kant van informatiebeveiliging en niet over technisch-inhoudelijke aspecten.

www.nictiz.nl
@nictiz

Betere zorg
door betere informatie

Nictiz