1 BELEID

We streven in alles wat wij doen naar continue verbetering. Dit geldt ook voor informatiebeveiliging. Hiervoor hebben wij beleid geformuleerd dat als kader geldt voor onze doelstellingen en de risicobeheersing. Via de PDCA cyclus zullen wij dit beleid periodiek toetsen en verbeteren.

1.1 Strategisch beleid

De directie van Spete.nl ICT Diensten B.V. kiest ervoor om het management van informatiebeveiliging in te richten volgens ISO 27001 en in lijn met de relevante wet- en regelgeving.

Iedere medewerker kent het belang van informatiebeveiliging en past dit toe binnen het eigen werkgebied. De Gouden Regels zijn hierbij het uitgangspunt. Kennis en expertise zijn essentieel voor een bestendige Informatiebeveiliging en moeten geborgd worden. Alle medewerkers worden getraind in bewustwording voor informatiebeveiliging en het gebruik van beveiligingsprocedures.

Op dit moment worden operationele beleidsregels nog vaak opgelegd door klanten. De komende jaren willen wij dit gaan omzetten naar een gestandaardiseerde set met principes en uitgangspunten. Om dit te ontwikkelen en blijven beheersen kiezen wij ervoor om onze diensten met Microsoft producten in te richten. Ook zullen wij onze beveiligingsniveaus toetsen aan de “best practices” van Microsoft.

1.2 Beleidsregels volgens ISO 27001, Annex A

Beleid voor mobiele apparatuur	Alle mobiele apparatuur is toegestaan, mits het apparaat is voorzien van actuele patches, anti-malware en bestandsencryptie.
Beleid voor telewerken	Telewerken is toegestaan met goedgekeurde apparatuur dat wil zeggen middels met een werkend antivirus pakket en een veilige internet verbinding. Openbare en/of Publieke netwerken zijn hierin niet toegestaan, met uitzondering van door Spete.nl ICT Diensten ingerichte apparatuur. De Remote Desktop verbinding naar de virtuele werkplek gaat middels remote gateway over een veilige verbindingen (SSL certificaat). Na een tweetrapsverificatie middels de applicatie DUO, logt de medewerker op zijn persoonlijke virtuele werkplek.

Beleid voor toegangsbeveiliging	Toegangsbeveiliging middels multi factor authenticatie op basis van best effort.
Beleid inzake het gebruik van cryptografische beheersmaatregelen	Transport- en dataencryptie op basis van classificatie.
'Clear desk'- en 'clear screen'-beleid	Clear screen & clear desk beleid geldt voor vertrouwelijke en geheime informatie, voor zowel fysieke als IT werkplekken
Back-up van informatie	Back-ups worden op basis van classificatie redundant uitgevoerd, bewaring (ook) buiten de fysieke locatie met minimaal 14 dagen retentie en een bijbehorend testschema
Beperkingen voor het installeren van software	Installatie van software mag alleen worden opgeslagen op de gescheiden, persoonlijke virtuele werkplek van de medewerker op basis van lokale administrator rechten.
Beleid en procedures voor informatietransport	Transport-, bericht- en dataencryptie via goedgekeurde informatietransportmiddelen op basis van classificatie.