

Bijlage Aantonen passend niveau van beveiliging

Normenstelsel

- ☐ De opdrachtnemer werkt volgens een algemeen erkende norm voor informatiebeveiliging, te weten:
..... (vermeld normenstelsel, zoals bijvoorbeeld NEN7510, NEN/ISO 27001, PCI/DSS)
en is volgens deze norm wel/niet gecertificeerd.
- ☐ De opdrachtnemer werkt volgens een algemeen erkende overheidsnorm zoals de BIO, of vergelijkbaar, te weten:,
- ☐ De opdrachtnemer werkt volgens een andere norm, te weten:
.....

Toereikendheid

De toereikendheid van de informatiebeveiliging blijkt uit het volgende:

- ☐ Opdrachtnemer verstrekt een actueel en geldig certificaat en verklaring van toepasselijkheid (VVT);
- ☐ Rapportages van periodieke externe controles zoals audits, pentesten of TPM's (bijv. ISAE3xxx SOC type II);
- ☐ Een assurance rapport (TPM) van een auditor die is aangesloten bij NOREA;
- ☐ Eigen controles of eigen mededelingen over de beveiligingsmaatregelen zoals hieronder beschreven (in lijn met de aanpak uit hoofdstuk 4.4 uit de BIO, een ICV):
.....

NB: Uit de certificering/periodieke externe controles/audits of uit de eigen controles/beschrijvingen blijkt of kan afgeleid worden dat de beveiliging passend is bij de verwerking(en) die gedaan worden.

Aansluiting bij goedgekeurde gedragscode

- ☐ Opdrachtnemer is aangesloten bij een door een toezichthoudende autoriteit goedgekeurde gedragscode, te weten