Thema Informatiebeveiliging

Nr	Vraag	Score	Advies
1	De organisatie beschikt over een gedocumenteerd informatiebeveiligingsbeleid	Niet of nauwelijks (0 % - 15 %)	*Informatie is één van de belangrijkste assets van iedere organisatie. Daarom dient informatie zeer zorgvuldig te worden beschermd tegen ontvreemding en misbruik. Het informatiebeveiligingsbeleid dient te worden gedocumenteerd.*
2	De verantwoordelijkheid voor informatiebeveiliging is op directieniveau vastgelegd	5,5	*Informatiebeveiliging is minstens zo belangrijk als beveiliging van andere eigendommen van uw organisatie. Daarom dient een directielid daarvoor verantwoordelijk te zijn.*
3	Het informatiebeveiligingsbeleid is door de directie goedgekeurd	5,5	*Vanwege de directieverantwoordelijkheid voor informatiebeveiliging, dient het informatiebeveiligingsbeleid door de directie te worden goedgekeurd.*
4	Heeft uw organisatie richtlijnen voor vertrouwelijkheid van Intellectueel Eigendom, gegevens en documenten	Niet of nauwelijks (0 % - 15 %)	*Richtlijnen voor vertrouwelijkheid van Intellectueel Eigendom, gegevens en documenten dienen te worden opgesteld, om collega's erop te wijzen dat zij daarmee zorgvuldig dienen om te gaan.*
5	Zijn de rollen en verantwoordelijkheden voor informatieclassificatie toegewezen	Gedeeltelijk (> 15 % - 50 %)	*Rollen en verantwoordelijkheden voor informatieclassificatie dienen te worden opgesteld, zodat duidelijk is welke informatie voor welke lezers toegankelijk is. Een veelgebruikte indeling: bestemd voor publiek, voor intern gebruik, of vertrouwelijk.*
6	Worden alle medewerkers in uw organisatie middels voorlichting en training geïnformeerd over het belang van informatiebeveiliging	Niet of nauwelijks (0 % - 15 %)	*Informatiebeveiliging vergt een proces van bewustwording. Een directeur of manager dient te worden vastgesteld die de verantwoording neemt voor voorlichting en training over informatiebeveiliging.*
7	Is de toegang tot uw bedrijfspand(en) beveiligd met een receptie en/of toegangscontrolesystemen	Grotendeels (> 50 % - 85 %)	*Het beveiligen van informatie begint met het beveiligen van uw bedrijfspand(en). Dit is minstens zo belangrijk als het nemen van IT-maatregelen. Wij raden aan dat u zich hierover laat voorlichten.*
8	Onze organisatie heeft maatregelen genomen ter voorkoming van ongeoorloofd meenemen van apparatuur	Grotendeels (> 50 % - 85 %)	*Het is vrij eenvoudig om een smart phone, laptop, tablet of pc te stelen van een bureau. Smart phones, laptops en tablets mogen niet eenvoudig door bezoek mee te nemen zijn.*
9	Wij beschikken over apparatuur die ongeoorloofde toegang tot ons netwerk detecteert en voorkomt	Niet of nauwelijks (0 % - 15 %)	*Installeer detectie-apparatuur die ongeoorloofde netwerktoegang vaststelt en voorkomt. Dit voorkomt dat bezoek apparatuur aansluit en inzicht krijgt in uw gegevens.*
10	De gebruikersorganisatie informeert ons adequaat en tijdig over instroom en vertrek van collega's	Gedeeltelijk (> 15 % - 50 %)	*Borg dat de IT-organisatie tijdig informatie ontvangt over personeelsmutaties, zodat toegangsrechten tijdig gemuteerd kunnen worden.*
11	Alle IT-medewerkers hebben een policy voor zorgvuldig en integer gebruik van hun IT-rechten ondertekend	Nee	*IT-personeel heeft veelal toegang tot veel informatie op het netwerk. Laat hen een policy ondertekenen waarmee zij zich bewust worden van integere omgang met deze rechten. Vermeld daarin ook de sanctie voor het geval IT-rechten worden misbruikt.*
12	Waren de afgelopen 12 maanden vrij van misbruik van autorisaties	Nee	*Analyseer het misbruik van autorisaties en voer preventieve maatregelen in.*
13	Voor het veilig uitwisselen van gegevens(dragers) zijn procedures opgesteld	Nee	*Stel procedures op om het uitwisselen van gegevens op media (zoals USB-sticks, harde schijven) of via dataverbindingen veilig te laten plaatsvinden.*
14	Eindgebruikers weten dat zij apparatuur niet onbeheerd mogen achterlaten (zoals laptops en mobiele telefoons)	5,5	*Stel een richtlijn op waarmee dit expliciet aan eindgebruikers wordt duidelijk gemaakt, en laat dit bijvoorbeeld door de afdeling personeelszaken aan nieuwe en bestaande medewerkers ondertekenen.*

