Format Informatiebeveiligingsbeleid

Inhoud

1. Inleiding

Voor u ligt het informatiebeveiligingsbeleid van Organisatie. Binnen dit beleid beschrijven wij de kaders van het informatiebeveiligingsbeleid en de visie die wij op informatiebeveiliging hebben.

Onder informatiebeveiliging wordt verstaan het treffen en onderhouden van een samenhangend pakket aan maatregelen om de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening te garanderen. De kwaliteitsaspecten:

- *Beschikbaarheid:* de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;
- *Integriteit*: de mate waarin gegevens of functionaliteit juist ingevuld zijn;
- *Vertrouwelijkheid:* de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Hierbij gaat het ook om de controleerbaarheid van de maatregelen die genomen zijn om deze kwaliteitsaspecten te borgen.

De directie verplicht zichzelf tot het naleven van de voorschriften volgens de ISO 27001:2013 en verklaart al het nodige te doen om het managementsysteem op te zetten en te implementeren, op peil te houden en de effectiviteit van het systeem daar waar nodig continue te verbeteren. De directie ziet er op toe dat de integriteit van het managementsysteem wordt gehandhaafd wanneer veranderingen worden doorgevoerd. Dit informatiebeveiligingsbeleid heeft een geldigheidsduur van 1 jaar. Daarna wordt het herzien.

Organisatie,

Datum

Naam directeur

2. Reikwijdte van het beleid

Dit document beschrijft het informatiebeveiligingsbeleid van Organisatie. De reikwijdte van ons beleid is…….

In de reikwijdte van het beleid wordt beschreven wat de afbakening is van het toepassingsgebied ervan. U geeft hier dus exact aan welke onderdelen / activiteiten onder de reikwijdte vallen. Een voorbeeld kan zijn:

"het beheer, transport en de veiligstelling van digitale bedrijfsinformatie van organisatie op tape, inclusief de levering van backup tapes en een eventuele vernietiging van de tape".

3. Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid heeft als doel het waarborgen van de continuïteit van de bedrijfsvoering en het minimaliseren van de schade door het voorkomen van beveiligingsincidenten en het minimaliseren van eventuele gevolgen.

Door het beter structureren van het informatiebeveiligingsbeleid bij Organisatie wordt aantoonbaar dat dit beleid bijdraagt aan de realisering van de missie die Organisatie voor zichzelf heeft geformuleerd ('alignment'). De missie is:

Hier komt uw missie.

Deze omgeving behoort veilig te zijn en te voldoen aan relevante wet- en regelgeving.

4. Beleidsuitgangspunten en – principes

Het management van informatiebeveiliging wordt als proces ingericht. Dat houdt in dat de jaarlijkse planning en controlecyclus, gebaseerd is op ISO 27001 (Plan, Do, Check, Act). Hierin worden jaarplannen opgesteld en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen.

De beleidsuitgangspunten bij Organisatie zijn:

- De beveiliging dient te voldoen aan de relevante wet- en regelgeving, in het bijzonder aan de Wet Bescherming Persoonsgegevens (2001).
- De beveiliging dient de volgende aspecten te waarborgen:
    - Beschikbaarheid
    - Integriteit
    - Vertrouwelijkheid.

Organisatie hanteert de volgende beleidsprincipes:

- Informatiebeveiliging is een **lijnverantwoordelijkheid:** dat betekent dat de lijnmanagers (afdelingshoofden) de primaire verantwoordelijk dragen voor een goede informatiebeveiliging op hun afdeling / eenheid. Dit omvat ook de keuze van maatregelen en de uitvoering en handhaving ervan.
- Informatiebeveiliging is **ieders verantwoordelijkheid**. Verwachtingen t.a.v. individuen: communiceer met medewerkers, klanten en derden dat er van hen verwacht wordt dat ze actief bijdragen aan de veiligheid van geautomatiseerde systemen en de daarin opgeslagen