* Het informatiebeveiligingsbeleid, of een verwijzing naar dit beleid
* De doelstellingen en de reikwijdte van dit plan
* De organisatie voor informatiebeveiliging, binnen de reikwijdte van dit plan
* De taak- en verantwoordelijkheidsverdeling
* De beveiligingseisen en -randvoorwaarden
* De risicos waartegen beveiliging nodig is
* De te nemen beveiligingsmaatregelen
* De richtlijnen en de planning voor implementatie en onderhoud van deze maatregelen
* De middelen die gebruikt worden voor informatiebeveiliging
* De risicos waarop de verschillende maatregelen invloed hebben
* De toetsing en evaluatie van de geimplementeerde maatregelen en de planning hiervoor
* De wijze waarop beveiligingsincidenten geregistreerd en afgehandeld worden
* Fallbackprocedures voor toepassing na een beveiligingsincident
* Opleidingsplan met betrekking tot informatiebeveiliging
* Een calamiteitenparagraaf

CATEGORIEN VOOR INFORMATIEBEVEILIGINGSPLAN

1. Beveiligingsbeleid
   1. Doelstellingen voor informatiebeveiliging vastleggen in het beleidsdocuemtn: beschrijving van dde te bereiken of na te streven situatie in termen van de bedrijfsbelangen. Het beleid wordt goedgekeurd en uitgedragen door het management
2. Organisatie van de beveiliging
   1. Beveiligingsfuncties, taken en verantwoordelijkheden, coordinatie, samenhang en rapportagelijnen. Verantwoordelijkheid voor afspraken voer samenwerking met derden
3. Classificatie en beheer van de bedrijfsmiddelen
   1. Overzicht van de bedrijfsmiddelen en hun verantwoordelijke eigenaar. Gebruik van classificatieschemas voor informatie, bijbehorende beveiligingsmaatregelen
4. Personeel
   1. Training, security awareness, veilig gedrag op de werkvloer, aannamebeleid en functioneringsbeoordeling. Reageren op en melden van beveiligingsincidenten
5. Fysieke beveiliging en omgeving
   1. Beveiliging van en in de infrastructuur. Toegangscontrole bij de poort, fysieke beveiliging van computerruimten en decentrale copmuters. Clear desk policy. Strommvoorziening, datacommunicatielijnen, koeling. Bescherming van diskettes, tapes en documentatie
6. Computer- en netwerkbeheer
   1. Bedieningsprocedures, beheer van de technische beveiliging en verantwoordelijkheden voor dit beheer. Antivirusmaatregelen, incidentafhandeling en -rapportage, beveiliging bij uitwisseling van gegevens, email, EDI
7. Toegangsbeveiliging
   1. Toegangsbeheersing en -autorisatie voor informatiesystemen
8. Ontwikkeling en onderhoud van systemen
   1. Aandacht voor de nodige beveiligignsfunctionaliteit en veilige ontwikkel- en onderhoudemethoden leiden ‘zeker’ tot veilige systemen, die ook veilig blijven (change management)
9. Continuiteitsplanning
   1. Calamiteitenopvang, rampenplannen, uitwijk
10. Toezicht
    1. Naleving van wettelijke en contractuele voorschriften, beveiligingscontrole op IT-systemen, IT-audit, interne controle