

# ea

# team

project teamwork  
relink life and work



## Informatiebeveiliging

Bijna wekelijks in het nieuws te horen, privacy gevoelige gegevens liggen op straat. Bedrijfsgegevens zijn per ongeluk uitgelekt en politieke geheimen staan op wikileaks! Hoe beschermen we onze privacy gevoelige gegevens en hoe kunnen we er van uit gaan dat belangrijke documenten alleen op de bedrijfsvloer te vinden zijn?

Wetgeving die de beveiliging van gegevens centraal stelt, zoals de WBP, is onvoldoende om de beveiliging van gegevens te garanderen. Innovatieve maatregelen moeten worden getroffen om de veiligheid van bedrijfsinformatie te waarborgen. Het belangrijkste uitgangspunt in informatiebeveiliging is het hanteren van een organisatiebreed informatiebeveiligingsbeleid.

## Relink life and work

Met overal en altijd toegang tot informatie, wordt werken en leven steeds meer één geheel. Bijvoorbeeld tijdens de zwemles van je zoon even zakelijke emails beantwoorden via de I Phone. Dit is ook de gedachte achter onze visie: 'Relink life and work'. Met het overal kunnen raadplegen van informatie moet natuurlijk ook goede informatievoorziening en –beveiliging gewaarborgd worden. Onze uitdaging is om goed gebruik van informatie te bevorderen, door niet alleen te vertrouwen op technische oplossingen en procedures maar ook door betrekken van menselijk gedrag (bewustmaking van risico's, normen en waarden, verantwoordelijkheden). Dit draagt bij aan een veilig informatieklimaat overal en altijd.

## Organisatiebrede implementatie een must voor iedere organisatie

Het beveiligen van informatie is niet alleen de toegangsbeveiliging van een systeem. De meeste informatiebeveiligingsincidenten ontstaan door personen. Een medewerker plaatst niet wetend informatie op internet of gegevens worden verstrekt aan personen die zich voordoen als een bekende. Om dergelijke informatiebeveiligingsincidenten te voorkomen wordt een beleid opgesteld waarin maatregelen worden getroffen.

len noodzakelijk zijn. De bronhouder legt deze maatregelen vast in een informatiebeveiligingsbeleid, waarna de maatregelen, indien nodig, worden geïmplementeerd.

## Beleid

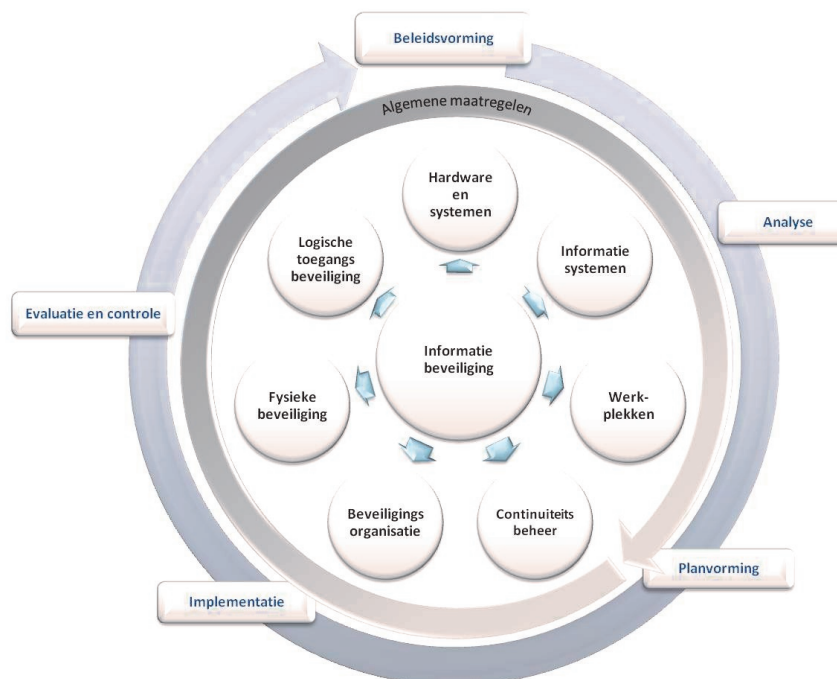
Een goed beleid bestaat zoals duidelijk wordt uit beleidsvorming, gevolgd door analyse, planvorming, implementatie van maatregelen en evaluatie en controle. Op basis van een jaarlijkse frequentie wordt deze cirkel van activiteiten herhaald.

## Werkprocessen

Maatregelen hebben veelal invloed op organisatiebrede werkprocessen. Maatregelen in het kader van informatiebeveiliging hebben effect op onder andere hardware, werkplekken, continuïteitsbeheer maar ook op fysieke beveiliging van het pand waarbinnen zich de informatie bevindt. Juiste implementatie van informatiebeveiliging zorgt voor integratie in de dagelijkse werkzaamheden.

## Basisregistraties

Binnen het informatiebeveiligingsbeleid is onder andere de door de overheid verplicht gestelde landelijke afname van basisgegevens een belangrijk punt van aandacht voor veel organisaties. De landelijke afname van basisgegevens is mede mogelijk doordat informatie digitaal wordt vastgelegd. De verantwoordelijkheid voor de beveiliging van deze gegevens blijft desondanks bij de bronhouder liggen. De beveiliging van deze basisregistraties kan worden gegarandeerd wanneer voor alle organisatieonderdelen risico's worden nagegaan waarvoor maatregelen



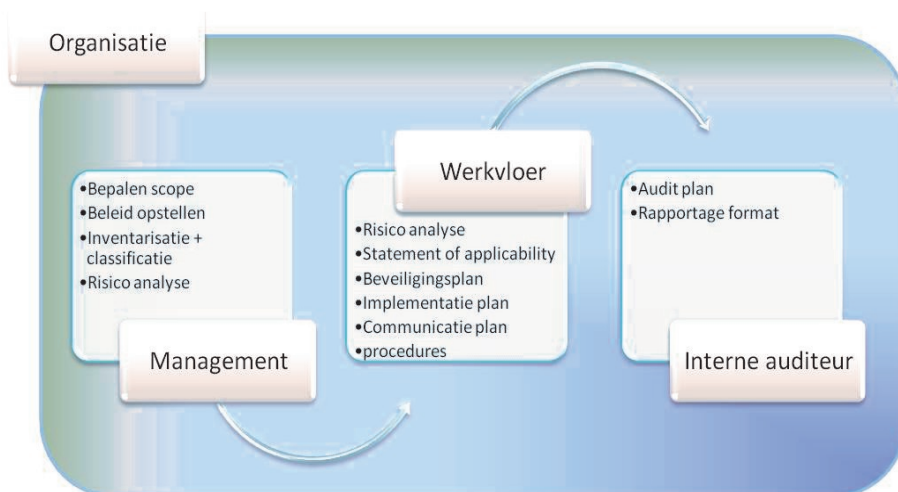
## Quickscan huidige situatie

Weet u waar uw organisatie staat voordat u een project rondom informatiebeveiliging start? Vooruitlopend op een project informatiebeveiliging of een traject naar ISO of NEN certificering kan Projectteamwork een nulmeting uitvoeren. In deze nulmeting wordt een analyse gemaakt van het huidige beveiligingsbeleid, de beveiligingsorganisatie, het beheer van informatiemiddelen, de fysieke beveiliging, het operationele beheer van

informatie en communicatievoorzieningen, toegangsbeveiliging, de beveiliging van werkplekken, continuïteitsbeheer en algemene maatregelen voor o.a. contracten en personeel. Met deze analyse kunt u een gedegen projectplan opstellen waarin een goede tijdsindicatie en de benodigde middelen kunnen worden vastgesteld.

## Intergrale aanpak & projectmanagement op basis van een resultaaterplichting

Projectteamwork hanteert een integrale aanpak bij de implementatie van informatiebeveiliging. Zowel het management als de werkvloer wordt betrokken bij het opzetten van het informatiebeveiligingsbeleid. Nadat er een duidelijk beeld is geschetst waar uw organisatie staat, kan gestart worden met de uitvoering van de invoering van informatiebeveiliging. Projectteamwork biedt u de mogelijkheid om op basis van een resultaatsverplichting u het werk uit handen te nemen. Wij verzorgen de gehele uitvoering van het informatiebeveiligingsproject inclusief het opstellen van de maatregelen en de uitvoering van het implementatieplan op basis van een vooraf afgesproken budget. Wij stellen (volgens de Prince 2 principes) een plan van aanpak op met daarin opgenomen de op te leveren resultaten, planning, organisatie en kwaliteit. In het plan van aanpak worden heldere procesafspraken gemaakt die van belang zijn tijdens de uitvoering van het project (zoals momenten voor besluitvorming).



## Uitvoering project

Het project informatiebeveiliging bestaat uit een aantal belangrijke speerpunten te weten:

### Denken

- Beleidsvorming
- Inventarisatie van informatiemiddelen
- Risico analyse
- Beveiligingsplan (de maatregelen)

### Doen

- Implementatieplan (technisch, organisatorisch en fysieke maatregelen)
- Communicatieplan
- Procedures (op een lean werkwijze)
- Audits

Belangrijk is om u te realiseren dat informatiebeveiliging de gehele organisaties treft. Immers de gehele organisatie maakt gebruik van informatie en onderhoudt systemen die van belang zijn voor de continuïteit, Het is belangrijk de gehele organisatie bij het project te betrekken middels goede communicatie in bijvoorbeeld de vorm van een postercampagne. Bij de uitvoering van het implementatieplan krijgt over het algemeen ook de gehele organisatie te maken met de verschillende maatregelen.

Wilt u meer weten over informatiebeveiliging of onze werkwijze, neem dan contact met ons op via [informatiebeveiliging@projectteamwork.nl](mailto:informatiebeveiliging@projectteamwork.nl)



**Projectteamwork**

**Bezoekadres:**

**Abe Lenstra Boulevard 62  
8448 JB Heerenveen**

**Postadres:**

**Rondgang 13  
8391 LN Noordwolde**

**T: 085 8640240**

**info@projectteamwork.nl  
www.projectteamwork.nl**