# Handboek Informatiebeveiliging

# conform ISO 27001 en NEN 7510

Bedrijfsnaam

Concept

# Voorwoord

Dit handboek informatiebeveiliging heeft als doel de werkwijze van het managementsysteem voor informatiebeveiliging (ISMS) inzichtelijk te maken voor betrokkenen. In dit handboek wordt verwezen naar van toepassing zijnde documentatie. Het handboek is beschikbaar voor medewerkers via het intranet. Bij vragen kan de Information Security Officer verduidelijking geven.

Het handboek volgt de volgende structuur:



# Documenthistorie

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Versie** | **Datum** | **Auteur(s)** | **Status** | **Beschrijving** |
| 0.1 | 2-11-2019 |  | Concept | Eerste opzet |
|  |  |  |  |  |
|  |  |  |  |  |

# Inhoudsopgave

[PLAN: Context van de organisatie 4](#_Toc23592070)

[Bedrijfsprofiel 4](#_Toc23592071)

[Scope – toepassingsgebied voor ISO 27001 en NEN 7510 4](#_Toc23592072)

[Organisatieschema 4](#_Toc23592073)

[Interne en externe factoren 4](#_Toc23592074)

[Belanghebbenden 5](#_Toc23592075)

[Wet- en regelgeving 5](#_Toc23592076)

[PLAN: Risicomanagement 5](#_Toc23592077)

[PLAN: Beleid en strategie 6](#_Toc23592078)

[Verantwoordelijkheid 6](#_Toc23592079)

[Borging 6](#_Toc23592080)

[PLAN: Doelstellingen 7](#_Toc23592081)

[PLAN: Planning 7](#_Toc23592082)

[DO: Uitvoering 8](#_Toc23592083)

[Personeel 8](#_Toc23592084)

[Voorafgaand aan het dienstverband 8](#_Toc23592085)

[Tijdens het dienstverband 8](#_Toc23592086)

[Beëindiging en wijziging van dienstverband 8](#_Toc23592087)

[Toegangsbeveiliging 9](#_Toc23592088)

[Informatiebeveiliging in projectbeheer 9](#_Toc23592089)

[Informatie classificatie 9](#_Toc23592090)

[Fysieke beveiliging 10](#_Toc23592091)

[Inkoop 10](#_Toc23592092)

[Uitbestede software ontwikkeling 10](#_Toc23592093)

[Beheer van bedrijfsmiddelen 10](#_Toc23592094)

[Apparatuur 11](#_Toc23592095)

[Plaatsing en bescherming van apparatuur 11](#_Toc23592096)

[Onderhoud 11](#_Toc23592097)

[Stroomvoorzieningen 11](#_Toc23592098)

[Beveiliging van bekabeling 11](#_Toc23592099)

[Bedrijfsvoering 11](#_Toc23592100)

[Procedures 11](#_Toc23592101)

[Incidentbeheer 12](#_Toc23592102)

[Documentatie beheer 12](#_Toc23592103)

[Wijzigingsbeheer 12](#_Toc23592104)

[Bescherming tegen malware 12](#_Toc23592105)

[Back-up en herstel 12](#_Toc23592106)

[Verwijderen van media 13](#_Toc23592107)

[Systeem- en netwerkarchitectuur 13](#_Toc23592108)

[Cryptografie 13](#_Toc23592109)

[Bedrijfscontinuïteit 14](#_Toc23592110)

[CHECK: Monitoren en evaluatie 15](#_Toc23592111)

[Monitoren en meten 15](#_Toc23592112)

[Logging 15](#_Toc23592113)

[Kwetsbaarheidstesten 15](#_Toc23592114)

[Overlegstructuur 16](#_Toc23592115)

[Interne audits 16](#_Toc23592116)

[Externe audits 17](#_Toc23592117)

[ACT: Verbeteren 17](#_Toc23592118)

# PLAN: Context van de organisatie

## Bedrijfsprofiel

Missie/visie

Producten/diensten

## Scope – toepassingsgebied voor ISO 27001 en NEN 7510

De scope van het managementsysteem voor informatiebeveiliging van Bedrijfsnaam is:

[invullen]

[Bedrijfsnaam]draagt zorg bij aan het beveiligen van informatie in relatie tot onze dienstverlening XYZ

Bij NEN 7510, de volgende zin bijvoegen:

Voor zorginstellingen en/of zorginformatie wordt in de Verklaring van Toepasselijkheid ISO of NEN….d.d. datum… versie XX gespecificeerd welke activiteiten, producten of diensten zijn uitbesteed en welke interfaces er bestaan.

## Organisatieschema

De organisatie ziet er als volgt uit: [organisatieschema]

Om de taken en verantwoordelijkheden voor informatiebeveiliging te kunnen uitvoeren is een aantal personen in de organisatie aangewezen. Er zijn verschillende taken en verantwoordelijkheden toegewezen aan verschillende personen in de rollenmatrix. De directie heeft de eindverantwoordelijkheid voor het systeem. De Security Officer heeft de belangrijkste rol in de uitvoering van het management systeem.

Conflicterende taken en verantwoordelijkheidsgebieden worden zoveel mogelijk gescheiden om de kans op onbevoegd en onbedoeld wijzigen of misbruik van de bedrijfsmiddelen van de organisatie te verkleinen.

Om de continuïteit van de organisatie te bevorderen heeft zorgt de organisatie dat alle processen van de organisatie door tenminste twee personen binnen de organisatie kunnen worden uitgevoerd. Dit is inzichtelijk gemaakt in de functie-vervangingsmatrix.

Referentie:

* ISMS tool (werkblad Rollen)
* Functieomschrijving Security Officer
* Functievervangingsmatrix

## Interne en externe factoren

De verschillende interne en externe factoren die van invloed zijn op het ISMS van Bedrijfsnaam zijn beschreven in de SWOT analyse. Deze factoren worden jaarlijks herzien en meegenomen tijdens de risicoanalyse.

Referentie:

* ISMS tool (werkblad SWOT)

## Belanghebbenden

In de ISMS tool (werkblad stakeholderanalyse) beschrijft Bedrijfsnaam de belanghebbenden die relevant zijn voor het managementsysteem voor informatiebeveiliging en de verwachtingen en contractuele eisen van én aan deze stakeholders. Wijzigingen worden minimaal één keer per jaar beoordeeld en bijgehouden in het document. Wanneer er acties voortvloeien uit wijzigingen worden die op de actielijst opgenomen en opgevolgd. [4.2]

Referentie:

* ISMS tool (werkblad Stakeholdersanalyse)

## Wet- en regelgeving

Bedrijfsnaam voldoet aan de van toepassing zijnde wet- en regelgeving op het gebied van informatiebeveiliging. Wijzigingen in wet- en regelgeving worden minimaal één keer per jaar beoordeeld en bijgehouden in het in de ISMS tool (werkblad wet- en regelgeving). Wij houden ons op de hoogte van wijzigingen door de bronnen beschreven in dit document. Wanneer er acties voortvloeien uit wijzigingen worden die op de actielijst opgenomen en opgevolgd. [4.2]

Referentie:

* ISMS tool (werkblad Wet- en regelgeving)

# PLAN: Risicomanagement

Risico’s en kansen voor het behalen van het gewenste informatiebeveiligingsniveau zijn geïnventariseerd in de ISMS tool (werkblad RAM). Op basis van de risicoanalyse worden gepaste maatregelen bepaald om de risico’s voor de beschikbaarheid, integriteit en vertrouwelijkheid van informatie tot een aanvaardbaar niveau terug te brengen. Zo kan tevens de prioriteit worden bepaald van de inzet van middelen en de volgorde waarin de maatregelen moeten worden geïmplementeerd.

Na de inventarisatie en evaluatie sessie dienen alle verantwoordelijke formele goedkeuring te geven over de risico’s en de scores die daarbij horen. Formele goedkeuring kan bijvoorbeeld via de notulen van een overleg of via een mail waar goedkeuring op gegeven wordt.

Referentie:

* Formele goedkeuring verantwoordelijken

De methode voor het bepalen van de risico score en de te volgen strategieën is tevens opgenomen in het werkblad “Methode RAM”.

Minimaal één keer per jaar wordt een volledig nieuwe risicoanalyse uitgevoerd. Daarnaast worden tussentijds urgente risico’s, die bijvoorbeeld zijn ontstaan door wijzigingen, voorgelegd tijdens overleggen. Indien nodig, zal de risicoanalyse worden bijgewerkt. [6.1; 8.2; 8.3]

Referentie:

* ISMS tool (werkblad Methode RAM)
* ISMS tool (werkblad RAM)

# PLAN: Beleid en strategie

Ondergetekende, de directie van Bedrijfsnaam, hecht grote waarde aan een adequate informatiebeveiliging binnen de organisatie.

Door de systematische zorg voor informatiebeveiliging wil Bedrijfsnaam op structurele wijze het volgende bereiken:

* Minimaliseren van bedrijfsimpact en financiële kosten van beveiligingsincidenten.
* Informatiebeveiligingsincidenten beheersbaar maken en houden.
* Voldoen aan relevante landelijke en Europese wet- en regelgeving.
* Tevreden opdrachtgevers, medewerkers en maatschappelijke omgeving.
* Verbeteren marktpositie.

## Verantwoordelijkheid

Om de genoemde doelstellingen te bereiken, is de inzet van alle medewerkers noodzakelijk. Regels en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn bekend bij alle medewerkers middels het personeelshandboek en worden verplicht getraind.

De eindverantwoordelijkheid voor informatiebeveiliging ligt bij de directie.

## Borging

De afspraken met betrekking tot de inrichting van het systeem voor informatiebeveiliging zijn vastgelegd in dit handboek. Dit systeem voldoet aan de eisen zoals omschreven in de ISO 27001 en NEN 7510 norm. Hiertoe wordt het systeem periodiek (minimaal jaarlijks) getoetst door een onafhankelijke deskundige.

Informatiebeveiliging is een continu verbeterproces volgens de plan-do-check-act cyclus. Daarom wordt het vastgestelde beleid conform de ISMS planning periodiek herijkt.

Het beleid is alleen te realiseren indien eenieder zich daarvoor inzet. De directie draagt er zorg voor dat dit beleid bij eenieder bekend is.

Door ondertekening van dit beleid geeft de directie goedkeuring aan dit beleid.

<Plaats, datum>

<handtekening>

De heer/Mevrouw NAAM

Directie Bedrijfsnaam

# PLAN: Doelstellingen

In het beleid is een aantal algemene doelen bepaald. Deze zijn vertaald naar specifieke meetbare doelstellingen. De status van de doelstellingen wordt voor aanvang van het security overleg in kaart gebracht en beoordeeld tijdens het overleg. Tijdens de <directiebeoordeling> worden de resultaten over het hele jaar geëvalueerd. De doelstellingen, en de status en realisatie ervan, zijn beschreven in de ISMS tool (werkblad Doelstellingen). [5.2; 6.2]

Referentie:

* ISMS tool (werkblad Doelstellingen)
* Notulen Directiebeoordeling
* Notulen security overleg

# PLAN: Planning

Om de uitvoering van de taken met betrekking tot informatiebeveiliging te borgen is een jaarplanning opgesteld.

Daarnaast wordt er voor elke drie jaar een interne audit planning vastgesteld.

Referentie:

* ISMS tool (werkblad ISMS planning)
* ISMS tool (werkblad Interne audit planning)

# DO: Uitvoering

## Personeel

### Voorafgaand aan het dienstverband

* Functieprofielen: De noodzakelijke competenties van de persoon die werkzaamheden voor de organisatie gaat verrichten worden vastgesteld. [7.2]
* Screening: Voorafgaand aan het dienstverband wordt de achtergrond van alle kandidaten geverifieerd conform de Checklist screening. [A.7.1.1]
* Arbeidsvoorwaarden: Werknemers ondertekenen voor de start van hun werkzaamheden een contract, waarin hun verantwoordelijkheden ten aanzien van informatiebeveiliging formeel zijn vastgelegd. [A.7.1.2]

Referentie:

* Functieprofielen
* Arbeidsovereenkomst

### Tijdens het dienstverband

* Indiensttredingsprocedure: Wanneer een medewerker in dienst komt, wordt de indiensttredingsprocedure gevolgd zoals is vastgesteld in de Checklist Indiensttreding. In deze checklist wordt onder andere verwezen naar de verstrekking van bedrijfsmiddelen en de verstrekking van autorisaties. [A.9.2.1]
* Iedere medewerker dient bij indiensttreding een toets met betrekking tot informatiebeveiliging met voldoende resultaat afronden.
* Verantwoordelijkheid van de directie: De directie eist van werknemers dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures zoals beschreven in het <personeelshandboek>. [A.7.2.1]
* Training en opleiding: Alle interne en externe werknemers van Bedrijfsnaam krijgen, voor zover relevant voor hun functie, geschikte training en regelmatige bijscholing met betrekking tot onder andere malware, beleid en procedures. [A.7.2.2]
* Disciplinaire procedure: Er is een formele disciplinair proces vastgesteld voor werknemers die inbreuk op informatiebeveiliging hebben gepleegd. Dit is vastgelegd in <> en gecommuniceerd met alle medewerkers. [A.7.2.3]

Referentie:

* Checklist indiensttreding
* Personeelshandboek

### Beëindiging en wijziging van dienstverband

* Uitdiensttredings- en functiewijzigingsprocedure: Wanneer een medewerker uit dienst treedt of van functie verandert, geldt het uitdiensttredings- of functiewijzigingsproces zoals is vastgesteld in de checklists. In deze checklists wordt onder andere verwezen naar de inname van bedrijfsmiddelen en het blokkeren van toegangsrechten. [A.8.1.4; A.9.2.1]

Referentie:

* Checklist functiewijziging
* Checklist uitdiensttreding

## Toegangsbeveiliging

Uitgangspunten met betrekking tot toegangsbeveiliging [A.9.1.1, A.9.4.1]:

* Toegang tot informatie en IT-faciliteiten zal op basis van ‘need to know’ worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie. [A.9.1.2]
* Het verstrekken van bevoorrechte toegangsrechten wordt beperkt.
* In de autorisatiematrix zijn per rol de rechten (fysiek en logisch) gedefinieerd.
* De autorisatiematrix is leidend bij het verlenen van toegang.
* Indien een medewerker meerdere rollen heeft en conflicterende rechten ontstaan, zijn de hoogst toegekende rechten geldig.
* Poorten, diensten en soortgelijke voorzieningen op een netwerk of computer die niet vereist zijn voor de dienst dienen te worden afgesloten. [A.9.1.2]
* Het op een correcte wijze verlenen en intrekken van autorisaties bij indiensttreding, functiewijziging en uitdiensttreding is geborgd middels de checklists indiensttreding, functiewijziging en uitdiensttreding.
* Toegangsrechten voor medewerkers van klanten worden alleen verstrekt wanneer deze zijn aangemeld door vertrouwde personen bij deze klanten, zoals vastgelegd in het document <>.
* Conform de ISMS planning worden de toegangsrechten van zowel medewerkers als medewerkers van klanten gecontroleerd.
* Toegang tot systemen en toepassingen wordt beheerst door een beveiligde inlogprocedure.
* Logische toegangsbeveiliging tot de omgeving middels gebruikersnaam en wachtwoord. Wachtwoorden dienen minimaal 6 karakters lang te zijn, minimale complexiteit te voldoen en minimaal eens per 90 dagen te worden gewijzigd.
* Het wachtwoordbeheer systeem waarborgt sterke wachtwoorden. [A.9.4.3]
* Het gebruik van systeemhulpmiddelen, zoals teamviewer, die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen wordt waar mogelijk beperkt. [A.9.4.4]

Referentie:

* + Overzicht beveiling (werkblad: autorisatiematrix)
	+ Checklist indiensttreding, uitdiensttreding en functiewijziging
	+ Document waarin vertrouwde personen bij klanten zijn vastgelegd

## Informatiebeveiliging in projectbeheer

Informatiebeveiliging komt aan de orde in ieder project van Bedrijfsnaam. Dit wordt geborgd middels de Project checklist. [A.6.1.5]

Referentie:

* Project checklist

## Informatie classificatie

De informatiebeveiliging van FLS Nederland, hangt af van de beschikbaarheids-, integriteits- en vertrouwelijkheidseisen van de informatie die wordt beschermd.

Om dit vast te kunnen stellen wordt er gebruik gemaakt van een classificatiemodel. In het classificatiemodel “Data classificatie” zijn de verschillende informatie-klassen binnen Bedrijfsnaam beschreven en is de informatie ingedeeld in deze klassen. Voor iedere klasse is beschreven hoe de informatie behandeld dient te worden. [A.8.2.1-A.8.2.3]

Referentie:

* Overzicht beveiliging (werkblad toelichting)
* Overzicht beveiliging (Data Classificatie)

## Fysieke beveiliging

In het Overzicht beveiliging (werkblad: Zones) zijn de zones van Bedrijfsnaam gedefinieerd en worden per zone geschikte beveiligingsmaatregelen genomen op basis van de classificatie van de informatie in deze zone. Deze zones worden jaarlijks beoordeeld. [A.11.1]

Referentie:

* Overzicht beveiliging (werkblad zones)

## Inkoop

Bij de aanschaf van nieuwe informatiesystemen of uitbreiding van bestaande informatiesystemen, die rechtstreeks effect hebben op het eindproduct of de dienst van de organisatie (bedrijf kritisch), worden de volgende stappen doorlopen [A.14.1.1]

* Vaststellen behoefte en bepalen of hier al (positieve) ervaring mee is in de eigen organisatie. Hierbij vanzelfsprekend rekening houdend met de informatiebeveiligingsaspecten en de wensen/eisen van onze eigen klanten, zoals ISO certificering, SLA, verwerkersovereenkomst.
	+ Bij positief resultaat: reeds bekende partner benchmarken ten opzichte van 1 of 2 alternatieven;
	+ Bij negatief resultaat: lijst samenstellen op basis van ervaringen van relaties en/of door marktonderzoek verkregen inzichten.
* Gesprekken voeren met leveranciers: uitsluitend wanneer de in te kopen dienst of product hierom vraagt. Afweging op basis van kosten en de vraag of het bedrijf kritische leverancier betreft.
* Leveranciersselectie: In de stakeholderanalyse is een lijst van de leveranciers van bedrijf kritische goederen/diensten opgenomen. Deze kritieke leveranciers worden minimaal jaarlijks beoordeeld. [A.15.2.1; A.15.2.2]
* **Onderhandelen en inkopen:** Aanschaffen van informatiesysteem.
* **Registratie:** De ingekochte middelen worden geregistreerd in het overzicht bedrijfsmiddelen.
* **Installeren:** Het plaatsen en installeren/inrichten van apparatuur en systeemprogrammatuur (al dan niet door de leverancier).
* **Testen:** wanneer nodig, wordt de werking van de ingekochte middelen getest alvorens in gebruik te worden genomen.

Referentie:

* ISMS tool (werkblad: Stakeholdersanalyse)
* Leveranciersbeoordeling

## Beheer van bedrijfsmiddelen

* Inventarisatie en eigendom: Alle bedrijfsmiddelen van Bedrijfsnaam die samenhangen met informatie en informatie verwerkende faciliteiten en de eigenaar van de bedrijfsmiddelen zijn geïnventariseerd in het Overzicht beveiliging (werkblad: Bedrijfsmiddelen) [A.8.1.1; A.8.1.2]
* Aanvaardbaar gebruik: De regels voor aanvaardbaar gebruik van bedrijfsmiddelen staan beschreven in het Personeelshandboek. [A.8.1.3]
* Teruggave: Teruggave van bedrijfsmiddelen is geborgd middels de checklist uitdiensttreding, zoals beschreven in 10.3. [A.8.1.4]

Referentie:

* Overzicht beveiliging (werkblad: Bedrijfsmiddelen)
* Personeelshandboek
* Checklist uitdiensttreding

## Apparatuur

### Plaatsing en bescherming van apparatuur

De volgende regels gelden voor apparatuur in computerruimtes (datacenters) [A.11.2.1]:

* Apparatuur wordt opgesteld en aangesloten conform de voorschriften van de leverancier. Dit geldt minimaal voor temperatuur en luchtvochtigheid, aarding, spanningsstabiliteit en overspanningsbeveiliging.
* Standaard accounts in apparatuur worden gewijzigd en de bijbehorende standaard leveranciers wachtwoorden worden gewijzigd bij ingebruikname van apparatuur.
* Gebouwen zijn beveiligd tegen de gevolgen van blikseminslag.
* Eten en drinken zijn verboden in serverruimtes.
* Een informatiesysteem dient te voldoen aan de hoogste classificatie-eisen, conform de informatie die voor kan komen op het informatiesysteem bij het verwerken ervan. Indien dit niet mogelijk is, wordt een gescheiden systeem gebruikt voor de informatieverwerking waaraan hogere eisen gesteld worden.

### Onderhoud

* Onderhoud gebeurt volgens de door de leverancier aanbevolen voorschriften en servicetijdstippen.
* Reparatie en onderhoud van apparatuur wordt alleen uitgevoerd door bevoegd onderhoudspersoneel.
* Er worden registraties bijgehouden van alle vermeende of daadwerkelijke storingen en van alle preventieve en corrigerende onderhoudswerkzaamheden. [A.11.2.4]

### Stroomvoorzieningen

Apparatuur is beschermd tegen stroomuitval middels [A.11.2.2]:

* ..

### Beveiliging van bekabeling

Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten zijn in ingericht in lijn met geldende “best practices” ter bescherming tegen interceptie, verstoring of schade. [A.11.2.3]

## Bedrijfsvoering

### Procedures

Verschillende primaire en ondersteunende activiteiten zijn vastgelegd in procedures en beschikbaar gesteld aan de gebruikers die ze nodig hebben. De procedures zijn voor medewerkers toegankelijk via <>. De procedures worden jaarlijks gecontroleerd op juistheid. [A.12.1.1]

Referentie:

* <Locatie procedures>

### Incidentbeheer

Wanneer zich incidenten, klachten of afwijkingen voordoen ten aanzien van informatiebeveiliging dienen deze te worden behandeld volgens de procedure incidentbeheer.

Referentie:

* Procedure incidentbeheer

### Software ontwikkeling

<…>

### Documentatie beheer

Bedrijfsnaam beheert haar gedocumenteerde ISMS informatie in elektronische vorm op <Platform>. De toegang tot de documenten komt overeen met het beleid voor toegangsbeveiliging. De documentatie wordt minimaal voorzien van een titel, datum, auteur, classificatie indien het classificatiebeleid dit vereist? en versieaanduiding. Om eenduidige documentatie te garanderen, wordt er gebruik gemaakt van excel en word sjablonen.

Oude versies van documenten worden minimaal één jaar bewaard. [7.5.3]

### Wijzigingsbeheer

Bedrijfsnaam hanteert de volgende uitgangspunten met betrekking tot veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatie beveiliging: [A.12.1.2]

* Veranderingen worden voor implementatie geregistreerd in systeem.
* Voor niet-standaard veranderingen wordt tijdens het teamoverleg de impact van de wijziging beoordeeld en worden de benodigde beveiligingsmaatregelen gespecificeerd.
* Wijzigingen die een verhoogd risico voor de informatiebeveiliging vormen worden eerst in een proefopstelling getest. De test en de testresultaten worden in de regel gedocumenteerd.
* Systemen voor ontwikkeling, test en acceptatie (OTA) zijn logisch gescheiden van Productie (P) om onbevoegde toegang tot of wijzigingen in productiesystemen te voorkomen. [A.12.1.4]
* Voor alle wijzigingen wordt formele goedkeuring verkregen door de opdrachtgever (veelal de

proceseigenaar).

* Waar mogelijk wordt de verandering voor implementatie gemeld aan gebruikers.

### Bescherming tegen malware

[A.12.2.1]

Beschrijf hier hoe data wordt beschermd tegen malware. Beschrijf ten minste:

* Technische maatregelen
* Creëren bewustwording bij medewerkers
* Verwijzing naar regels in personeelshandboek

Referentie:

* Personeelshandboek

### Back-up en herstel

Alle systemen, databases en bestanden in het datacenter van Bedrijfsnaam worden geback-upt en daarnaast is er sprake van redundantie.

[A.12.3.1]

Beschrijf in de procedure het back-up plan. Beschrijf ten minste:

* Wie is verantwoordelijk voor:
	+ Uitvoering back-ups
	+ Gegevensherstel
	+ Monitoring
* Frequentie back-ups
* Verwijzing naar back-up en herstel procedure
* Back-up tests
	+ Frequentie
	+ Wie is verantwoordelijk
* Back-ups worden bewaard op een andere locatie dan de oorspronkelijke data, om te voorkomen een incident op de oorspronkelijke locatie niet leidt tot schade aan de back-up.
* De fysieke toegangsbeveiliging van de back-ups is gelijk aan die van de oorspronkelijke data***.***

Referentie:

* Back-up en herstel procedure

### Verwijderen van media

Wanneer (apparatuur met) opslagmedia niet langer nodig zijn voor Bedrijfsnaam dient te worden gewaarborgd dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of veilig zijn overgeschreven.

Beschrijf procedure van de organisatie.

[A.8.3.2; A.11.2.7]

Referentie:

* Overzicht beveiliging (werkblad: Data classificatie)

## Systeem- en netwerkarchitectuur

Het netwerk van Bedrijfsnaam en de netwerken waarover gegevens worden uitgewisseld dienen in voldoende mate te zijn beveiligd. Bedrijfsnaam hanteert vijf principes in de netwerkbeveiliging:

1. Redundantie: Het redundant uitvoeren van (kritieke) netwerkcomponenten. [A.17.2.1]
2. Diversiteit: Het toepassen van meervoudige beveiligingsmechanismen.
3. Isolatie: Het netwerk zo inrichten dat delen ervan kunnen worden geïsoleerd.
4. Veilige Defaults: Al het onbekende verkeer is geblokkeerd en alle netwerkcomponenten, zoals routers en firewalls, zijn op de juiste manier geconfigureerd.
5. Beperkingen: Het toevoegen van privilege beperkingen en encryptie op (gevoelige) informatie op het netwerk.

 Bedrijfsnaam onderhoudt een netwerktekening waarin de beveiligingsmaatregelen worden getoond.

Beschrijf eventueel de interne en externe systeem- en netwerkarchitectuur. [A.13.1.1 – A.13.1.3]

Referentie:

* Netwerktekening

## Cryptografie

Voor encryptie van informatie hanteren wij de volgende uitgangspunten [A.10.1.1]:

* Encryptie is in ieder geval van toepassing op zowel de opslag als het transport van vertrouwelijke informatie.
* Op harde schijven en verwijderbare media op alle systemen moet volledige encryptie worden toegepast, ongeacht de classificatie van de informatie die er op staat.
* Beveiligingsmaatregelen in relatie tot encryptie worden aangegeven in het classificatiemodel.
* Bij het gebruik van encryptie wordt de wet- en regelgeving in acht genomen.
* De eigenaar van de informatie is verantwoordelijk voor de encryptie van de informatie.

**Sleutelbeheer** [A.10.1.2]

Referentie:

* Overzicht beveiliging (werkblad: Data classificatie)

## Bedrijfscontinuïteit

Om de bedrijfscontinuïteit van Bedrijfsnaam in het geval van een calamiteit te waarborgen, is een Bedrijfscontinuïteitsplan opgesteld. Er worden minimaal jaarlijks oefeningen en testen gehouden om het plan te toetsen. Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold. [A.17.1.1-A.17.1.3]

Voor een optimale beschikbaarheid zijn componenten, zoals stroom en koeling, redundant uitgevoerd. [A.17.2.1]

Referentie:

* Continuïteitsplan Bedrijfsnaam
* Testrapport bedrijfscontinuïteitsplan

# CHECK: Monitoren en evaluatie

## Monitoren en meten

De organisatie evalueert de informatiebeveiligingsprestaties en de doeltreffendheid van het managementsysteem voor informatiebeveiliging door op verschillende wijzen te monitoren en meten, zoals onder andere de capaciteit [A.12.1.3]. In het werkblad Monitoren en meten (ISMS tool) staat beschreven wat de organisatie monitort en op welke manier dit gebeurt.

De resultaten van het monitoren en meten worden geanalyseerd voorafgaand aan het security overleg door de verantwoordelijke personen. Dit wordt vervolgens geëvalueerd tijdens <security overleg>. Acties die daaruit voorkomen worden opgenomen op de actielijst. Tijdens de directiebeoordeling wordt gekeken naar de bijzonderheden over het gehele jaar. [9.1]

Referentie:

* ISMS tool (werkblad Monitoren en meten)
* Notulen Security Overleg
* Notulen Directiebeoordeling

## Logging

Om achteraf inzicht te kunnen verkrijgen in een bepaalde gebeurtenis dienen gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen te worden vastgelegd. Hiertoe worden op diverse niveaus en locaties logs bijgehouden:

* ..
* ..

Voor een juiste tijdwaarneming worden alle netwerkonderdelen voorzien van een centrale tijdsynchronisatie via het NTP protocol.

De informatie in de logbestanden is beschermd middels toegangsrechten. Daarnaast zijn in de logging oplossing maatregelen genomen om te voorkomen dat beheerders geregistreerde logging informatie bewerken of verwijderen.

De logging wordt geanalyseerd voorafgaand aan het security overleg door de verantwoordelijke personen. Dit wordt vervolgens geëvalueerd tijdens <security overleg>. Acties die daaruit voorkomen worden opgenomen op de actielijst. Tijdens de directiebeoordeling wordt gekeken naar de bijzonderheden over het gehele jaar. [A.12.3.1; A.12.4.1]

## Kwetsbaarheidstesten

Om te onderzoeken of de technische beheersmaatregelen effectief zijn ingericht wordt er conform de ISMS planning een kwetsbaarheidstest uitgevoerd. De bevindingen zullen middels een rapportage met de directie worden gecommuniceerd. Afwijkingen en geïnitieerde verbeterpunten zullen door de directie worden beoordeeld en bij acceptatie zullen de te nemen acties worden opgenomen in de actielijst. [A.18.2.3]

Om de bedrijfsprocessen zo min mogelijk te verstoren, zijn de rechten tijdens de audits beperkt tot alleen-lezen-toegang tot software en gegevens. Bovendien worden auditactiviteiten die de beschikbaarheid van systemen kunnen beïnvloeden uitgevoerd buiten werkuren. [A.12.7.1]

Referentie:

* ISMS tool (werkblad: ISMS planning)
* Rapport kwetsbaarheidstest

## Overlegstructuur

Om de informatiebeveiliging te kunnen evalueren/beoordelen en te verbeteren zijn er de volgende overleggen:

|  |  |  |  |
| --- | --- | --- | --- |
| **Overleg** | **Frequentie** | **Aanwezig** | **Onderwerpen** |
| Werkoverleg | 4 x per jaar | * Alle medewerkers
 | * Doornemen beleid en procedures
* Verbetermogelijkheden informatiebeveiliging
* Uitkomsten security overleg doornemen
 |
| Security overleg | 4 x per jaar | * Directie
* Security Officer
* …
 | * Status actielijst
* Beoordelen actualiteit documentatie
* Evalueren incidenten
* Evalueren monitoring en loggegevens
* Evalueren doelstellingen
* Evalueren back-up herstel test
* Evalueren test bedrijfscontinuïteitsplan
* Bewustzijn medewerkers
* Actualiteiten informatiebeveiliging
 |
| Directiebeoordeling | 1 x per jaar | * Directie
* Security Officer
 | * Acties voorgaande overleg
* Wijzigingen in interne/externe factoren
* Wijzigingen in wet- en regelgeving
* Risicomanagement
* Stakeholdermanagement
* Resultaten van monitoren en meten
* Incidenten
* Informatiebeveiligingsdoelstellingen
* Evaluatie van leveranciers
* Middelen
* Personeel
* Auditresultaten
* Verbeteren - actiepunten
 |

## Interne audits

Om te onderzoeken of het ISMS en de bijbehorende beheersmaatregelen effectief zijn ingericht om geïdentificeerde risico’s in voldoende mate te beheersen en of er nog ongenoemde risico’s zijn die voor de organisatie van belang zijn, wordt er jaarlijks een interne audit uitgevoerd aan de hand van de planning. De organisatie stelt hiervoor elke drie jaar een interne audit planning vast.

Om objectiviteit te waarborgen, voert een externe partij de interne audits voor ons uit. De interne audit wordt uitgevoerd door iemand die tenminste voldoet aan onderstaande competenties:

* Kennis van de ISO 27001 norm
* Bekend met audit methode
* Objectief en onpartijdig

Van de interne audits wordt een rapport gemaakt, dat naar de directie wordt gecommuniceerd. Afwijkingen en geïnitieerde verbeterpunten zullen door de directie worden beoordeeld tijdens de directiebeoordeling en bij acceptatie zullen de te nemen acties worden opgenomen in de actielijst. [9.2; A.18.2.1]

Referentie:

* ISMS tool (werkblad: Interne audit planning)
* Rapportage interne audit

## Externe audits

Om de werking, effectiviteit en de conformiteit van het informatiebeveiligingssysteem met de ISO 27001 en NEN 7510 norm te toetsen, wordt er jaarlijks een externe audit uitgevoerd. Hiermee wordt de informatiebeveiliging op een onafhankelijke wijze beoordeeld en geborgd.

# ACT: Verbeteren

Om structureel te kunnen verbeteren worden acties genoteerd en voorzien van een deadline en verantwoordelijke. De notulen van de overleggen geven acties weer en zorgen dat zij worden opgevolgd in een volgend overleg. Daarnaast hanteert Bedrijfsnaam een actielijst. Actie kunnen onder andere voortkomen uit de overleggen, audits en risicoanalyse. Via de registratie worden ze beheerst opgevolgd. Tijdens de directiebeoordeling wordt actielijst beoordeeld. [10]

Referentie:

* ISMS tool (werkblad: Actielijst)