

Interne procedures voor Informatiebeveiliging

[BEDRIJF]

Versie: [MAAND] 2021 [VERSIE]

Goedgekeurd door management: NOG NIET GOEDGEKEURD

## Inhoudsopgave

Inzicht in context en organisatie 5

Context en toepassingsgebied / scope 5

Issues en belanghebbenden 5

Leiderschap 6

Ondersteuning 7

Risico inschatting en -behandeling 8

Uitvoering 9

Evaluatie van de prestaties 10

Meten en monitoren 10

Interne audit 10

Directiebeoordeling 10

Verbetering 11

Reageren op afwijkingen 11

Continue verbetering 11

Informatiebeveiligingsbeleid (A5) 12

Aansturing door de directie van de informatiebeveiliging 12

Organiseren van informatiebeveiliging (A6) 13

Interne organisatie 13

Mobiele apparatuur en telewerken 14

Veilig personeel (A7) 16

Voorafgaand aan het dienstverband 16

Tijdens het dienstverband: 16

Beëindiging en wijziging van dienstverband 17

Beheer van bedrijfsmiddelen (A8) 18

Informatieclassificatie 18

Behandelen van media 19

Toegangsbeveiliging (A9) 20

Bedrijfseisen voor toegangsbeveiliging 20

Beheer van toegangsrechten van gebruikers 20

Gebruikersverantwoordelijkheden 21

Toegangsbeveiliging van systeem en toepassing 21

Cryptografie / versleuteling (A10) 23

Cryptografische beheersmaatregelen 23

Fysieke beveiliging en beveiliging van de omgeving(A11) 24

Beveiligde gebieden 24

Apparatuur 25

Beveiliging bedrijfsvoering (A12) 27

Bedieningsprocedures en verantwoordelijkheden 27

Bescherming tegen malware 27

Back-up 27

Verslaglegging en monitoren 28

Beheersing van operationele software 28

Beheer van technische kwetsbaarheden 28

Communicatiebeveiliging (A13) 30

Beheer van netwerkbeveiliging 30

Informatietransport 30

Acquisitie, ontwikkeling en onderhoud van informatiesystemen (A14) 32

Beveiligingseisen voor informatiesystemen 32

Beveiliging in ontwikkelings- en ondersteunende processen 32

Testgegevens 33

Leveranciersrelaties (A15) 34

Informatiebeveiliging in leveranciersrelaties 34

Beheer van dienstverlening van leveranciers 34

Beheer van informatiebeveiligingsincidenten (A16) 35

Beheer van informatiebeveiligingsincidenten en -verbeteringen 35

Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (A17) 37

Informatiebeveiligingscontinuïteit 37

Redundante componenten 37

Naleving (A18) 38

Naleving van wettelijke en contractuele eisen 38

Informatiebeveiligingsbeoordelingen 39

Bijlage: Procedure meldplicht datalekken 40

Bijlage: bezoekersregistratie 42

# Over dit document

Informatiebeveiliging is uitermate belangrijk voor onze organisatie, om fraude, bedrijfsonderbrekingen of gegevensverlies te voorkomen. Het management heeft besloten een informatiebeveiligingsbeleid aan te nemen met een aantal belangrijke maatregelen. Sommige van deze maatregelen zijn van toepassing op alle personeelsleden en worden beschreven in de personeelsrichtlijnen. Andere maatregelen zijn relevant voor specifieke beveiligingsrollen. Deze maatregelen worden beschreven in dit document. Dit document beschrijft per maatregel wat er moet gebeuren en wie verantwoordelijk is. Voor elke maatregel is een verantwoordelijke persoon en optioneel een back-up aangegeven.

Dit document maakt onderdeel uit van het [BEDRIJF] Information Security Management System (ISMS), een integrale aanpak van informatiebeveiliging. Voor meer details over dit ISMS, zie het document [BEDRIJF] Informatiebeveiligingsbeleid.

Dit document is opgezet als een centrale plaats waar alle procedures instaan. Iedereen die een procedure uitvoert moet dus bij dit document kunnen. Dit zijn bijvoorbeeld afdelingshoofden, IT-medewerkers en ook HR- of administratieve medewerkers. Dit document mag binnen [BEDRIJF] vrij worden verspreid. Het is niet bedoeld voor externe partijen.

Dit document wordt minimaal eens per jaar herzien. Het information security team houdt een werkversie bij met verbetervoorstellen. In de management­review wordt deze nieuwe versie aan directie gepresenteerd en geaccordeerd. Dit document wordt vervolgens aan alle betrokkenen verspreid.

Deze versie is goedgekeurd in [MAAND\_GOEDKEURING] [JAAR\_GOEDKEURING] en geldt tot er een nieuwe versie is of tot en met [MAAND\_GELDIG] [JAAR\_GELDIG].

#### Structuur

Dit document volgt de hoofdstukken-structuur van ISO 27002. Deze standaard is genummerd van A5 tot A18. Binnen elk hoofdstuk is de inhoud afgestemd op [BEDRIJF].

Aan het einde zijn een aantal appendices toegevoegd. Dit zijn concrete werkinstructies voor specifieke processen. De volgorde is willekeurig.

***Over dit template:***

*Dit template is gemaakt door de mensen van ICT Institute.*

*Het template mag gratis worden gebruikt, onder een creative commons licentie*

[*https://creativecommons.org/licenses/by/4.0/*](https://creativecommons.org/licenses/by/4.0/)

*De nieuwste versie staat op:*

[*https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/*](https://softwarezaken.nl/2022/01/gratis-27001-avg-templates/)

*Je mag het template uitbreiden, aanpassen en bewerken zoveel je wilt*

*Je mag het template en documenten gemaakt met het template doorgeven en delen zoveel je wilt*

*Als je het template doorgeeft, dan moet je "gemaakt door de mensen van ICT Institute" laten staan*

*Als je een document maakt met dit template en je bent geen opdrachtgever van ons, zet dat "gemaakt met template van ICT Institute" ergens in het document*

*Als je een opdrachtgever bent van ICT Institute, dan mag je alles doen met dit template wat je wilt*

*Let op dat je de ISO 27001 norm moet kopen bij NEN of een andere organisatie voordat je de norm gaat gebruiken. De norm is auteursrechtelijk beschermd*

*Lees vooral ook deze artikelen als je aan de slag gaat:*

[*https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/*](https://softwarezaken.nl/2017/03/samenvatting-iso-27001-informatie-beveiliging/)

[*https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/*](https://softwarezaken.nl/2021/12/iso-27001-certificatie-aanvraag/)

[*https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/*](https://softwarezaken.nl/2018/01/gdpr-avg-in-10-stappen/)

[*https://softwarezaken.nl/security-verified/*](https://softwarezaken.nl/security-verified/)

# Inzicht in context en organisatie

## Context en toepassingsgebied / scope

Deze is vastgelegd in het beleid.

## Issues en belanghebbenden

De organisatie stelt jaarlijks interne en externe issues vast en legt deze vast in een register. Ook worden de stakeholders (belanghebbenden) en hun eisen en verwachtingen vastgesteld. Dit is input voor risico-management.

# Leiderschap

De directie toont leiderschap en betrokkenheid bij het ISMS. Dit wordt onder andere gedaan door:

* Eindverantwoordelijkheid te nemen voor het ISMS
* Zorgen dat beleid en doelstellingen worden vastgesteld
* Zorgen dat de ISMS-eisen in de organisatie worden geïntegreerd
* Het zorgen voor voldoende menskracht en middelen
* Communiceren van het belang van het ISMS
* Zorgen dat doelen worden gehaald
* Actieve deelname aan training en overleggen van het ISMS
* Deel te nemen aan de directiebeoordeling
* Het bevorderen van continue verbetering
* De managers te ondersteunen om hun leiderschap te tonen binnen hun

verantwoordelijkheidsgebieden

De directie stelt het Informatiebeveiligingsbeleid vast en zorgt dat het passend is voor de organisatie, doelstellingen bevat of een kader voor vaststellen doelstellingen, een commitment om te voldoen aan eisen en om continue te verbeteren.

Het beleid wordt beschikbaar gesteld op de website en gecommuniceerd aan stakeholders wanneer nodig.

De directie wijst rollen en verantwoordelijkheden aan voor informatiebeveiliging. Deze zijn vastgelegd in dit handboek, sectie A6.

# Ondersteuning

De directie stelt middelen beschikbaar om de doelstellingen van het ISMS te bereiken. Dit blijk onder andere uit de gedefinieerde rollen en alle in dit handboek omschreven maatregelen

In dit handboek (A6) zijn rollen gedefinieerd die voor het ISMS noodzakelijk zijn. De benodigde competenties zijn gedefinieerd.

Er is een terugkerende awarenesstraining opgenomen in de jaarplanning. Nieuwe medewerkers krijgen ook een passende awareness-training.

Het InfoSec Team heeft hiervoor een regelmatig overleg (zie jaarplanning). Hierin wordt het volgende besproken:

* Incidenten: Zijn er incidenten geweest de afgelopen tijd en zijn passende acties gepland?
* Veranderingen: Zijn er nieuwe projecten, veranderingen of contracten waar het InfoSec Team naar moet kijken
* Jaarplanning: Welke activiteiten staan er voor afgelopen maand gepland in de jaarplanning? Zijn deze gepland en uitgevoerd?
* Monitoren en meten: Zijn er doelstellingen of KPI's die afgelopen maand of komende maand moeten worden geëvalueerd? Wat zijn de resultaten?
* Afwijkingen: Zijn er nieuwe afwijkingen? Worden er correctieve acties goed uitgevoerd op auditbevindingen of andere afwijkingen?

Beheer van documentatie: alle ISMS-documenten worden digitaal opgeslagen op een manier dat ze toegankelijk zijn voor de mensen die er bij moeten kunnen. Alle documenten hebben een versie, eigenaar en datum.

# Risico inschatting en -behandeling

Het IB-team gebruikt een methodologie voor continue verbetering. Met behulp van deze methodiek is het beveiligingsteam op de hoogte van de bedrijfsdoelen, definieert het acties, controleert het of de acties effectief zijn en brengt het veranderingen aan indien nodig. De gekozen methode is Plan-Do-Check-Act, een bekende methodiek die ook wel de

Deming-cyclus (<https://en.wikipedia.org/wiki/PDCA>) genoemd wordt.

De methodiek wordt op meerdere niveaus toegepast. Allereerst is het vertegenwoordigd op de agenda van de kwartaalvergaderingen. Ten tweede zijn er pre-audits, PEN-tests en andere aanvullende controles. In deze aanvullende controles controleert iemand buiten het IB-team of zelfs buiten onze organisatie of het IB-team effectief is en beveelt het indien nodig verdere acties aan voor het management. Ten slotte wordt het mechanisme ook op kleine schaal gebruikt, waarbij een deel van elke security vergadering suggesties moet bevatten om die vergadering effectiever te maken. Dit element is aanwezig in de kwartaalvergadering en in personeelsopleidingen / workshops.

Voor de identificatie en aanpak van risico's gebruiken wij een risicobeheermethodologie waarbij risico's worden ingedeeld op basis van hun impact en waarschijnlijkheid. Hierin staat de methode verder uitgewerkt. Het risico-overzicht bevat ook een behandelplan, bestaande uit beheersmaatregelen voor significante risico's.

Het [BEDRIJF] asset-inventaris wordt in het [DOC\_NAAM] -document onderhouden door het informatiebeveiligingsteam. Ons bedrijf gebruikt veel informatie-assets die beschermd moeten worden. Het ISMS-lijstdocument [DOC\_NAAM] biedt een overzicht van de assets die in onze organisatie worden gebruikt. Dit overzicht is gemaakt door management en medewerkers van het bedrijf, en wordt regelmatig bijgewerkt.

Voor elke informatie-asset in scope heeft dit beleid tot doel de volgende beveiligings- aspecten te verzekeren:

- Vertrouwelijkheid

- Integriteit

- Beschikbaarheid

# Uitvoering

Onze organisatie heeft een InfoSec Team dat de uitvoering van ISMS-acties monitort en zorgt dat doelen worden gehaald. Dit wordt gedaan door:

* Opstellen en volgen jaarplanning
* Bijhouden doelstellingen
* Bespreken van lopende acties en zaken in het InfoSec Teamoverleg.

In de overleggen wordt besproken of zaken goed lopen en eventueel maatregelen getroffen.

# Evaluatie van de prestaties

## Meten en monitoren

Er is een document “Doelstellingen en monitoren” waarin is vastgelegd welke zaken worden gemeten, inclusief hoe vaak en door wie.

## Interne audit

(verplicht voor ISO 27001, niet voor security verified) De organisatie heeft een interne auditor aangesteld die jaarlijks interne audits uitvoert om informatie te verkrijgen of het managementsysteem voor informatiebeveiliging overeenkomt met de eigen eisen van het managementsysteem voor informatiebeveiliging; en de eisen van ISO 27001 en of het doeltreffend is geïmplementeerd

## Directiebeoordeling

(verplicht voor ISO 27001, niet voor security verified) De organisatie voert jaarlijks een directiebeoordeling uit waarin de directie het managementsysteem voor informatiebeveiliging van de organisatie beoordeelt, om de continue geschiktheid, adequaatheid en doeltre doeltreffendheid te bewerkstelligen. Hierin worden de volgende zaken besproken:

* de status van acties als gevolg van voorgaande directiebeoordelingen;
* wijzigingen in externe en interne onderwerpen die relevant zijn voor het
* managementsysteem voor informatiebeveiliging;
* feedback over de informatiebeveiligingsprestaties, met inbegrip van trends in:
* afwijkingen en corrigerende maatregelen; resultaten van monitoren en
* meten; auditresultaten; en voldoen aan informatiebeveiligingsdoelstellingen;
* feedback van belanghebbenden;
* resultaten van risicobeoordeling en de status van het risicobehandelplan; en
* kansen voor continue verbetering.

Beslissingen van directie worden in een verslag vastgelegd.

# Verbetering

## Reageren op afwijkingen

De organisatie legt alle voor het ISMS belangrijke afwijkingen vast in een Register afwijkingen en correctieve maatregelen-H10.xlsx. Het InfoSec Team vult het register aan en zorgt dat er op de afwijking wordt gereageerd, deze wordt beoordeeld, grondoorzaken worden geëvalueerd en corrigerende maatregelen worden getroffen.

Afwijken kunnen geconstateerd worden tijdens:

* Monitoren en meten (9.1)
* Interne audits (9.2)
* Directiebeoordeling (9.3)
* Leveranciersbeoordeling (A15.2.1)
* Pen-testen (A12.6.1)
* Systeemtesten (A14.2.8)
* Privacy-audits
* Interne meldingen
* Externe certificatie audits

## Continue verbetering

Zowel de directie als het InfoSec Team spannen zich in om continue te blijven verbeteren, en nemen dit bijvoorbeeld mee in werkoverleggen, onderlinge gesprekken en contacten met andere medewerkers.

# Informatiebeveiligingsbeleid (A5)

## Aansturing door de directie van de informatiebeveiliging

#### 5.1.1 Beleidsregels voor informatiebeveiliging

We hebben een informatiebeveiligingsbeleid, genaamd [NAAM DOCUMENT]. Het is het hoofddocument van ons ISMS dat linkt naar de procedures, InfoSec-regels, Verklaring van Toepasselijkheid, risicoregister, assetregister en incidentenregister. Het bevat de context, doelen, reikwijdte van ons ISMS, een stakeholderanalyse en informatie over leiderschap, risicobeoordeling en -behandeling, assets, bewustzijn, training, operaties, prestatie-evaluatie en natuurlijk ons streven naar continue verbetering.

#### 5.1.2 Beoordelen van het informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid wordt aan het begin van elk jaar beoordeeld (vóór [MAAND] van elk jaar). Als de behoefte ontstaat, kan het beleid ook tussendoor herzien worden. Dit kan het geval zijn na een beveiligingsincident of grote wijziging in organisatiestructuur of -processen.

# Organiseren van informatiebeveiliging (A6)

### Interne organisatie

#### 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Het gehele management is op de hoogte van het informatiebeveiligingsbeleid en is vastbesloten om deze inspanning op permanente basis te ondersteunen. [BEDR\_VERANTW] is de managementvertegenwoordiger die rechtstreeks in contact staat met het informatiebeveiligingsteam. Er is een informatiebeveiligingsteam dat verantwoordelijk is voor het implementeren en onderhouden van informatiebeveiliging. Het team bestaat uit de volgende mensen:

1. A

2. B

3. C

De volgende taakomschrijving zijn belangrijk voor het ISMS:

|  |  |  |
| --- | --- | --- |
| Rol | Verantwoordelijkheid | Rol-eisen m.b.t. IB |
| CEO/algemeen directeur | Eindverantwoordelijk informatiebeveiliging. Vaststellen doelen en beleid  | Opleiding?X jaar ervaring in een leidinggevende functie |
| CISO  | Bijhouden van het ISMS om aan doelen en beleid te voldoen. Rapporteren status ISMS aan directeur | Afgeronde HBO- of academische opleiding Ervaring met IB-audits. |
| Privacy Officer  | Controle op naleving AVG. Afhandeling datalekken en privacyvragen / verzoeken  | CIPP/E of andere afgeronde privacytraining |
| CTO | Beheerder van externe IT-diensten. Verlenen / controleren rollen en rechten. | X jaar ervaring in een technische functie |
| HR verantwoordelijk | Verantwoordelijk voor medewerker screening en on/off-boarding | HR-opleiding |
| Interne auditor  | Uitvoeren van jaarlijkse interne audit | Ervaring met IB-audits.ISO 27001 lead auditor training |
| Alle medewerkers  | Kennen en naleven van de beleidsregels informatiebeveiliging |  |

Alle andere personeelsleden van het bedrijf worden regelmatig geïnformeerd door het informatiebeveiligingsteam en zijn verantwoordelijk voor het volgen van het beleid en de richtlijnen.

In document [ROLBESCHRIJVINGEN\_DOCUMENT] zijn rollen en verantwoordelijkheden verder uitgewerkt (met name inhoudelijk). Deze teksten zullen worden gebruikt bij vacatures.

#### 6.1.2 Scheiding van taken

Om misbruik van bedrijfsmiddelen te voorkomen, ligt de "macht" om een gevoelige activiteit volledig onder controle te houden niet bij dezelfde persoon. Dit wordt geïmplementeerd door alle activiteiten te loggen en belangrijke taken te splitsen, bijvoorbeeld in doen en controleren of goedkeuren en starten.

Vanwege de beperkte omvang van ons bedrijf is volledige segregatie moeilijk. Alle belangrijke functies (bijvoorbeeld toegang tot een bankrekening, bronbeheer) worden echter gedeeld door twee of meer personen. Dit wordt gedaan door de IT-admin en de directeur.

#### 6.1.3 Contact met overheidsinstanties

Contact met autoriteiten, bijvoorbeeld in het geval van het melden van crimineel gedrag, wordt afgehandeld door het management. [ROL] is bijvoorbeeld verantwoordelijk voor het melden van datalekken.

Contacten met overheidsinstanties zijn als volgt:

* Belastingdienst: directeur
* Autoriteit Persoonsgegevens: privacy officer
* Politie bij aangifte diefstal: directeur

#### 6.1.4 Contact met speciale belangengroepen

Het informatiebeveiligingsteam zorgt ervoor dat ze op de hoogte zijn van ontwikkelingen door:

* De beveiligingsgroep voor informatiebeveiliging NL: https://www.linkedin.com/groups/13533313/
* B
* C

#### 6.1.5 Informatiebeveiliging in projectbeheer

Om een succesvolle organisatie-brede ISMS-implementatie te verzekeren, wordt informatiebeveiliging in alle projecten overwogen en gedocumenteerd. Voor elke verandering in organisatieprocessen wordt een plan gemaakt. Het plan moet de volgende secties bevatten:

* Beschrijving van projectdoelen.
* Veranderingen in het ISMS die nodig zijn.
* Beveiligingsmaatregelen in geval van belangrijke productwijzigingen.
* Privacy als nieuwe persoonlijke gegevens worden verzameld of persoonlijke gegevens op een nieuwe manier worden gebruikt.
* Of een DPIA nodig is.

### Mobiele apparatuur en telewerken

#### 6.2.1 Beleid voor mobiele apparatuur

Veel mensen hebben hun eigen persoonlijke laptops, tablets en smartphones en gebruiken deze om informatie te delen. Het is technisch mogelijk om deze apparaten te gebruiken voor werkgerelateerde zaken, maar dit brengt ernstige veiligheidsrisico's met zich mee. [BEDRIJF] vraagt daarom zijn werknemers:

* Als ze een e-mailaccount van een bedrijf hebben, om het persoonlijke e-mailaccount niet te gebruiken voor werkgerelateerde e-mails.
* Om te zorgen dat elk apparaat van een respectabele fabrikant is, met een wachtwoord is beveiligd, vrij van malware en virussen is en regelmatig wordt bijgewerkt. Dit is voor hun eigen bescherming en als een extra voorzorgsmaatregel in het geval dat werkgerelateerde informatie naar een persoonlijk apparaat lekt.

#### 6.2.2 Telewerken

Medewerkers moeten alleen bekende en beveiligde netwerken gebruiken. Wanneer ze in openbare ruimtes werken, moeten ze expliciet het netwerk controleren waarmee ze verbonden zijn. Een bekend netwerk is het bedrijfsnetwerk of je thuisnetwerk. Als je op openbare netwerken moét werken, gebruik dan alleen SSL-beveiligde websites. Bij telefoongesprekken in openbare ruimtes mogen geen bedrijfsnamen of vertrouwelijke gegevens genoemd worden.

# Veilig personeel (A7)

### Voorafgaand aan het dienstverband

#### 7.1.1 Screening

De HR-verantwoordelijke is verplicht om een arbeidsovereenkomst (inclusief tijdelijke contracten en stagecontracten) volgens het afgesproken template op te stellen en zorgt ervoor dat elk contract de naleving van de personeelsrichtlijnen omvat. De HR-verantwoordelijke controleert ook of voor functies, waar dit van toepassing is, een Verklarig-omroep Gedrag wordt aangevraagd of dat referenties worden nagetrokken. De VOGs dienen de volgende categorieën te bevatten voor de volgende functieniveaus:

|  |  |
| --- | --- |
| **Functieniveau** | **Categorie geselecteerd** |
| Stagiair | Informatie |
| Hoger management | … |
| C-level directie | Informatie, Geld, Diensten, Zak. trans., Proces, Aanst. org. |
| Bestuursleden | … |

Tijdens het onboarding-proces wordt een checklist gebruikt om ervoor te zorgen dat alleen geschikte werknemers worden aangenomen, werknemers worden voorzien van geregistreerde apparaten, de juiste documentatie wordt gelezen en ondertekend en dat ze toegang krijgen volgens het Least Privilege-principe en op basis van Need to Know volgens ons toegangsbeleid. [LINK CHECKLIST ON-BOARDING]

#### 7.1.2 Arbeidsvoorwaarden

De contracten van de medewerkers bevatten een link naar HR-procedures en het IB-beleid van de organisatie, en welke rol de medewerker erin vervult. Toekomstige werknemers moeten hiervan op de hoogte worden gesteld en moeten in hun contract tekenen voor naleving ervan.

### Tijdens het dienstverband:

#### 7.2.1 Directieverantwoordelijkheden

Het management zorgt ervoor dat alle werknemers en contractanten op de hoogte zijn van het informatiebeveiligingsbeleid van het bedrijf en dit ook volgen. Ze leiden door middel van een voorbeeld en laten zien dat informatiebeveiliging zowel nuttig als noodzakelijk is.

#### 7.2.2 Bewustwording tijdens het dienstverband

[ROL] zorgt er ook voor dat elke persoon in de eerste week een training of instructie voor informatiebeveiliging ontvangt. Er wordt minstens één keer per jaar een bewustmakingstraining georganiseerd en je moet een dergelijke training bijwonen in de eerste werkweek bij deze organisatie en minstens één keer per jaar. De training is verplicht voor al het personeel dat met informatie in aanraking komt. Als werknemers geen training hebben gehad, moeten ze contact opnemen met de Security Officer.

#### 7.2.3 Disciplinaire procedure

Het niet naleven van deze richtlijnen zal leiden tot disciplinaire maatregelen zoals formele waarschuwingen, schorsing of ontslag. [BEDRIJF] beoordeelt gevallen per stuk.

**Belangrijk:** dit betekent niet dat je “gestraft wordt voor alle kleine ongelukjes”. Integendeel. Incidenten gebeuren en kunnen alleen worden opgelost als de juiste mensen hiervan op de hoogte zijn. Alleen grove nalatigheid en opzettelijke acties zullen leiden tot disciplinaire maatregelen.

### Beëindiging en wijziging van dienstverband

#### 7.3.1 Beëindiging of wijziging van verantwoordelijkheden van het dienstverband

Als werknemers het bedrijf verlaten (bijvoorbeeld einde contract of einde dienstverband), moeten ze het volgende doen:

* Lever alle apparaten en informatiedragers van het bedrijf in.
* Lever alle documenten in die vertrouwelijke gegevens bevatten (of verwijder deze op een veilige manier).
* Wis alle bedrijfsgegevens van privéapparaten die ze tijdens hun dienstverband hebben gebruikt.

De HR-verantwoordelijke draagt er zorg voor dat:

* Het gebruikersaccount uitgeschakeld is en is aangemerkt voor verwijdering
* Alle interne en externe forwarding van het mailaccount uitgeschakeld is
* Externe SaaS-accounts verwijderd zijn of intern overgedragen zijn

Zelfs na het einde van het contract zijn medewerkers nog steeds verplicht om informatie veilig te houden: ze mogen geen gevoelige of vertrouwelijke gegevens openbaar maken aan buitenstaanders na vertrek uit het bedrijf.

Als een medewerker van functie verandert, zorgt de HR-verantwoordelijke ervoor dat het volgende wordt gedaan:

* De VOG-categorieën worden opnieuw geëvalueerd en indien nodig geactualiseerd
* Toegangsmachtigingen worden bijgewerkt volgens het toegangsbeleid, waarbij rekening wordt gehouden met Least Privilege en Need to Know
* Sleutels worden ingeleverd en/of extra sleutels verstrekt aan de medewerker
* Het toegangsgebied van de tag (toegangsfob) is bijgewerkt

Voor elk einde van het dienstverband en elke interne verandering van het dienstverband wordt de checklist ([CHECKLIST OFFBOARDING AND SWITCH]) ingevuld door de HR- verantwoordelijke.

# Beheer van bedrijfsmiddelen (A8)

#### 8.1.1 Inventariseren van bedrijfsmiddelen

Ons bedrijf gebruikt veel informatie-items die moeten worden beschermd. Het ISMS-lijstdocument [DOC\_NAAM] biedt een overzicht van de assets die in dit bedrijf worden gebruikt. Dit overzicht is gemaakt door management en medewerkers van het bedrijf, en wordt regelmatig bijgewerkt. Voor elke informatie-asset in scope, heeft dit beleid tot doel de volgende beveiligingsaspecten te verzekeren:

* Vertrouwelijkheid
* Integriteit
* Beschikbaarheid

#### 8.1.2 Eigendom van bedrijfsmiddelen

Alle assets in de inventaris, dus van het hele bedrijf als de inventaris compleet is, hebben een eigenaar. Dankzij asset-eigendom worden assets gedurende hun hele levenscyclus bewaakt en onderhouden. Vergelijkbare assets worden gegroepeerd en het dagelijkse toezicht op een asset kan worden overgelaten aan een zogeheten custodian, maar de eigenaar blijft verantwoordelijk. Het eigenaarschap van assets moet worden goedgekeurd door het management.

#### 8.1.3 Aanvaardbaar gebruik maken van bedrijfsmiddelen

Gebruikers van de assets dienen er zorg voor te dragen de assets verantwoordelijk te gebruiken. Regels voor het aanvaardbaar gebruik van deze assets is te vinden in [DOCUMENT].

#### 8.1.4 Teruggeven van bedrijfsmiddelen

Wanneer een werknemer of externe partij geen toegang meer dient te hebben tot een asset vanwege bijvoorbeeld het einde van het dienstverband van de overeenkomst, moet deze het asset terugleveren aan [BEDRIJF]. Daar is een duidelijk beleid voor, dat door alle betrokkenen moet worden gekend. Niet-tastbare assets die belangrijk zijn voor de huidige activiteiten, zoals specifieke kennis die nog niet is gedocumenteerd, moeten worden gedocumenteerd en als zodanig worden geretourneerd.

### Informatieclassificatie

#### 8.2.1 Classificatie van informatie

Bepaalde informatie wordt als gevoelig beschouwd vanwege b.v. monetaire of juridische waarde, en moet vertrouwelijk blijven, terwijl andere informatie minder cruciaal is. [BEDRIJF] heeft een beleid ingesteld voor het omgaan met geclassificeerde informatie. De verantwoordelijkheid voor het classificeren van informatie-assets ligt bij de eigenaar. Om onderscheid te maken tussen het belang van verschillende geclassificeerde assets, is het volgende onderscheid gemaakt:

* Openbaar
* Intern gebruik
* Vertrouwelijk

Als je niet zeker weet in welke categorie een document of asset valt, vraag het dan aan je manager! We hebben liever meerdere keren dezelfde vraag dan dat een intern of vertrouwelijk document openbaar wordt gemaakt.

#### 8.2.2 Informatie labelen

Er is een classificatiematrix opgesteld

[invullen matrix]

*(ALS MEDISCHE DATA VERWERKT WORDT)*

Alle patiëntinformatie dient als Vertrouwelijk gelabeld te worden.

#### 8.2.3 Behandelen van bedrijfsmiddelen

Gebruikers van de assets dienen zorg te dragen om assets op een verantwoordelijke manier te gebruiken op basis van de gegeven classificatie. Vertrouwelijke documenten moeten worden opgeslagen in afgesloten kasten.

De drie soorten informatie moeten op de volgende manier worden behandeld:

**Openbare informatie:**

Informatie die al openbaar is, kan vrijelijk worden gedeeld met klanten en anderen. De informatie is vaak zelfs bedoeld om te worden gedeeld, zoals marketingmateriaal of onze normale contactgegevens. [VERDERE VOORBEELDEN VAN OPENBARE INFORMATIE]

**Voor intern gebruik:**

Interne documenten bevatten informatie die voor ons een specifieke zakelijke of strategische waarde heeft. Documenten zoals deze procedures, werkroosters, agenda's en interne telefoonnummers zijn niet bedoeld om extern bekend te zijn en gebruikt te worden door buitenstaanders. [VERDERE VOORBEELDEN VAN DOCUMENTEN VOOR INTERN GEBRUIK]

**Vertrouwelijk:**

Vertrouwelijke informatie moet, zoals de naam suggereert, vertrouwelijk blijven. Het heeft een hoge zakelijke, strategische of persoonlijke waarde en kan ernstige schade toebrengen aan [ORGANISATIE] of een persoon als het in verkeerde handen terechtkomt. [EXTRA REGELS VOOR HET WERKEN MET VERTROUWELIJKE INFORMATIE]. [VERDERE VOORBEELDEN VAN VERTROUWELIJKE DOCUMENTEN] Als een document een handtekening van een manager (van ons of van een ander bedrijf) of klant bevat, is het document hoogstwaarschijnlijk vertrouwelijk.

### Behandelen van media

#### 8.3.1 Beheer van verwijderbare media

Bedrijfsgegevens mogen niet worden opgeslagen op usb-sticks. Verwisselbare media kunnen alleen worden gebruikt met uitdrukkelijke toestemming van de Security Officer.

#### 8.3.2 Verwijderen van media

Wanneer media niet langer nodig is, wordt het op de juiste manier verwijderd om het lekken van data te voorkomen. Om te zorgen dat niets verloren gaat, documenteren we de vernietiging van media. Gevoelige media worden door het informatiebeveiligingsteam met extra zorg vernietigd. Mediaschrijven gebruikt in clouddiensten wort door de cloud provider gereinigd volgens de contractuele afspraken.

#### 8.3.3 Media fysiek overdragen

Media wordt niet fysiek overgedragen.

# Toegangsbeveiliging (A9)

### Bedrijfseisen voor toegangsbeveiliging

#### 9.1.1 Beleid voor toegangsbeveiliging

Medewerkers krijgen toegang van het management op basis van hun rol volgens het Least Privilege principe.

Geplande verbetering: [BEDRIJF] zal een matrix ontwikkelen die beschrijft welke toegang nodig is voor welke rol. Deze matrix wordt jaarlijks gereviewd door management.

#### 9.1.2 Toegang tot netwerken en netwerkdiensten

Gasten zijn niet toegestaan op het [BEDRIJF] -netwerk. Er is een afzonderlijk [GEBOUW] (gebouw) netwerk.

### Beheer van toegangsrechten van gebruikers

#### 9.2.1 Registratie en uitschrijven van gebruikers

Bij indiensttreding zorgt de HR-verantwoordelijke ervoor dat een account voor de nieuwe medewerker aangemaakt wordt. De medewerker krijgt de rechten zoals beschreven in de toegangsmatrix.

#### 9.2.2 Gebruikers toegang verlenen

De HR-verantwoordelijke wijzigt- of trekt de toegangsrechten binnen een week nadat een persoon vertrekt of van rol verandert in. In de offboarding checklist wordt genoteerd welke rechten ingetrokken zijn bij uitdiensttreding. In het geval van gedeelde wachtwoorden worden wachtwoorden actief gewijzigd.

#### 9.2.3 Beheren van speciale toegangsrechten

Beheerderstoegang en andere onbeperkte toegang (bijvoorbeeld database-wachtwoorden) wordt alleen gegeven aan een zeer beperkte reeks actieve beheerders die aanvullende instructies hebben ontvangen. Deze zijn gereserveerd voor platformbeheerders of IT-beheerders. Men kan in de platformdatabase bekijken wie platformbeheerder is.

Andere gebruikers worden alleen voorzien van normale, niet-beheerdersaccounts.

#### 9.2.4 Beheer van geheime authenticatie-informatie van gebruikers

Gegenereerde wachtwoorden moeten veilig worden gegenereerd en worden bevestigd aan de beste werkwijzen (zie 9.1.3). De toegangscontrole-verantwoordelijke is verantwoordelijk voor het controleren of alle systemen toegangscontrole hebben (bijvoorbeeld pin, biometrie of wachtwoord) en eisen dat toegangscontrole is ingeschakeld. 2-factor-authenticatie wordt zoveel mogelijk gebruikt. Het moet worden gebruikt voor [SOFTWARE].

#### 9.2.5 Beoordeling van toegangsrechten van gebruikers

Asset-eigenaren controleren regelmatig wie toegang tot hun bedrijfsmiddel heeft en welke rol wordt gewijzigd of waardoor een toegangsrechtenbeoordeling door het management wordt geactiveerd, bijvoorbeeld in [SERVICE], [SOFTWARE]. Platformbeheerrechten worden beoordeeld in de kwartaalevaluatie.

#### 9.2.6 Toegangsrechten intrekken of aanpassen

Zodra een contract of overeenkomst is beëindigd, worden de toegangsrechten van de ontvangende partij verwijderd. Als volledige verwijdering niet nodig is vanwege een voortzetting van een bepaalde soort, kunnen de rechten worden gewijzigd in plaats van worden verwijderd.

### Gebruikersverantwoordelijkheden

#### 9.3.1 Geheime authenticatie-informatie gebruiken

Wachtwoord en PIN (persoonlijk identificatienummer) beveiliging is een belangrijk aspect van alle beveiliging. Voor alle werkgerelateerde wachtwoorden moeten werknemers de volgende regels volgen:

* Voor elke dienst moeten werknemers een nieuw wachtwoord kiezen dat niet eerder is gebruikt of voor een andere service;
* Wachtwoorden moeten niet gemakkelijk te raden zijn, dus geen namen, verjaardagen of gewone woorden en geen wachtwoorden van minder dan 8 tekens;
* Wachtwoorden moeten minstens één keer per jaar worden gewijzigd;
* Persoonlijke wachtwoorden en accounts kunnen niet met anderen worden gedeeld;
* Medewerkers moeten hun wachtwoorden op een veilige manier bewaren, bijvoorbeeld een wachtwoordbeheerder gebruiken. [BEDRIJF] heeft [PASSWORD\_MANAGER] geselecteerd voor gedeelde informatie. Medewerkers kunnen de Security Officer om meer informatie vragen over het installeren en gebruiken van [PASSWORD\_MANAGER]. Gebruik van alternatieve services zoals [ANDERE\_SERVICE] wordt geaccepteerd;
* Medewerkers mogen wachtwoorden niet zichtbaar op de werkplek achterlaten. Als apparaten zoals mobiele apparaten de mogelijkheid hebben om een ​​pincode in te stellen voor apparaat toegang, is het verplicht om een ​​pincode van ten minste 6 cijfers in te stellen.

Dezelfde regels die van toepassing zijn op wachtwoorden (vers, niet zichtbaar) zijn van toepassing op pincodes.

### Toegangsbeveiliging van systeem en toepassing

#### 9.4.1 Beperking toegang tot informatie

[BEDRIJF] heeft een beleid voor toegangsrechten dat bepaalt dat toegang tot bepaalde systemen, middelen of informatie beperkt moet zijn. Deze toegangsrechten worden in de praktijk op precies dezelfde manier beperkt. Toegang wordt beoordeeld in de kwartaalevaluatie.

#### 9.4.2 Beveiligde inlogprocedures

Het beleid inzake toegangsrechten bepaalt dat toegang tot systemen is beveiligd en hoe gebruikers zich kunnen aanmelden.

#### 9.4.3 Systeem voor wachtwoordbeheer

[BEDRIJF] maakt gebruik van het [PASSWORD\_MANAGER] wachtwoordbeheersysteem.

#### 9.4.4 Speciale systeemhulpmiddelen gebruiken

Programma's die bevoorrechte toegang tot assets of systemen bieden, worden strak beheerd. Vanwege de mogelijkheden om besturingselementen en toegang tot een deel van een systeem dat de prestaties kan beïnvloeden, te onderdrukken, is hun gebruik zo beperkt mogelijk.

#### 9.4.5 Toegangsbeveiliging op programmabroncode

Alle broncode wordt opgeslagen in [STORAGE\_OPSLAG]. De broncode van interne applicaties kan op geen enkele manier toegankelijk zijn voor onbevoegd personeel en bevoegd personeel wordt regelmatig gecontroleerd en beoordeeld.

####

####

# Cryptografie / versleuteling (A10)

### Cryptografische beheersmaatregelen

#### 10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Aangezien sommige informatie vertrouwelijk moet blijven voor degenen die niet met het beheer zijn belast en de integriteit / authenticiteit ervan behouden moet worden, moet deze worden versleuteld. Voor dit soort situaties is het beveiligingsbeleid voor cryptografie ingesteld. In dit beleid staat vermeld wanneer cryptografische besturingselementen nodig zijn en welke typen in welke situaties passen.

De volgende versleuteling is verplicht:

* Gebruik van https voor alle webverkeer;
* Alle servers moeten minstens A in SSL-labs scoren: <https://www.ssllabs.com>;
* Voor e-mailbeveiliging wordt er regelmatig gecontroleerd met <https://internet.nl>.  Hierbij moet een score van minimaal [SCORE] worden gehaald;
* Voor de opslag op laptops en telefoons wordt ook encryptie gebruikt. Dit gaat met Bitlocker of de door Apple ingebouwde mogelijkheden.

Alle gegevens moeten zowel “in rest” als “in transit” versleuteld worden.

#### 10.1.2 Sleutelbeheer

[BEDRIJF] maakt gebruik van [ENCRYPTIE\_CERTIFICAAT]. Deze worden door [PROGRAMMA] aangemaakt en daar bijgehouden. Wijzigingen worden door de websitebeheerder gedaan. Het beleid is om de richtlijnen en adviezen van [PROGRAMMA] te volgen en de certificaten niet te exporteren.

Sleutels en wachtwoorden moeten voldoen aan de gestelde wachtwoordeisen. Bij voorkeur worden nieuwe wachtwoorden, met name voor adminaccouncts, gegenereerd via een programma dat is ontworpen voor het genereren van veilige sleutels. Bij voorkeur zijn dit, voor encryptie-toepassingen, random gegenereerde strings van 12 of meer tekens.

Wachtwoorden en andere sleutels moeten veilig worden opgeslagen in een wachtwoordbeheerder programma of op een andere veilige plaats. Zorg ervoor dat elke sleutel toegankelijk is voor ten minste twee personen om verlies van data of assets te voorkomen.

Gedeelde sleutels worden minstens jaarlijks gewijzigd en vaker wanneer sleutelpersoneel vertrekt.

# Fysieke beveiliging en beveiliging van de omgeving(A11)

### Beveiligde gebieden

#### 11.1.1 Fysieke beveiligingszone

Er is één hoofdbeveiligingszone, de kantoorruimte. De kamer is vergrendeld als deze niet in gebruik is en heeft een alarm.

[VOEG PLATTEGROND VAN KANTOOR MET ZONES IN]

In de hoofdruimte van het kantoor is een afgesloten kast voor gevoelige fysieke documenten en andere bedrijfsmiddelen. De servers en netwerkapparatuur staat in een afgesloten ruimte, die met een sleutel betreden kan worden vanuit het kantoor. Het kantoor zelf is af te sluiten met een sleutel, die in het bezit is van alle medewerkers.

Het kantoor bevindt zich in een gebouw met een gedeelde receptie, waar alle bezoekers zich moeten melden. Er is cameratoezicht in de gedeelde ruimtes, en ’s nachts heeft het gebouw bemande bewaking. Buiten werktijden is er een keycard nodig om het gebouw te betreden.

#### 11.1.2 Fysieke toegangsbeveiliging

Beveiligde gebieden zijn afgesloten van gemeenschappelijke ruimtes en de toegang daartoe is geautoriseerd en gedocumenteerd. Niet-personeel zoals bezoekers worden vergezeld en hun identiteit wordt gecheckt.

Alle medewerkers hebben een keycard om het gebouw buiten werktijden te betreden.

#### 11.1.3 Kantoren, ruimten en faciliteiten beveiligen

Elke beveiligingszone moet fysieke beveiliging hebben op zijn plaats, in de vorm van een fysieke of elektronische vergrendeling. De persoon die als laatste het kantoor verlaat moet er zeker van zijn om altijd te controleren of:

* alle vensters zijn gesloten;
* de deur is op slot;
* het alarm is ingeschakeld;
* alle elektronische apparaten zijn uitgeschakeld.

#### 11.1.4 Beschermen tegen bedreigingen van buitenaf

De fysieke externe en omgevingsgerelateerde risico’s zijn voor [BEDRIJF] laag. Alle data is opgeslagen in de cloud, en de servers op kantoor zijn slechts een back-up. Alle medewerkers zijn volledig uitgerust om thuis te werken.

#### 11.1.5 Werken in beveiligde gebieden

De enige beveiligde zone bij [BEDRIJF] is de serverruimte. Hiervoor is een speciale sleutel nodig, die alleen bij [ROLLEN] in bezit zijn. De sleutels tot de afgesloten kast zijn alleen in bezit van [ROLLEN]. Medewerkers die niet geautoriseerd zijn om de beveiligde zone of kast te betreden, mogen alleen onder begeleiding van een geautoriseerde collega tijdelijk toegang hebben.

#### 11.1.6 Laad- en loslocatie

Om (onbedoelde) ongeoorloofde toegang tot andere delen van de organisatie te voorkomen, vindt de levering plaats bij de receptie of bij een medewerker thuis. Gevoelige pakketten worden bij voorkeur op kantoor bezorgd, en bij thuisbezorging nooit bij de buren achtergelaten.

### Apparatuur

#### 11.2.1 Plaatsing en bescherming van apparatuur

Als er niemand op kantoor is, is het kantoor gesloten. Laptops, telefoons, en documenten mogen niet in het zicht blijven liggen als het kantoor gesloten is. Alle gevoelige documenten en informatiedragers dienen in de gesloten kast gelegd te worden.

De cloudprovider [PROVIDER] zorgt voor passende fysieke bescherming van de servers. Dit is vastgelegd in het contract. In onze eigen serverruimte worden geen fysieke documenten of andere brandbare spullen opgeslagen. De serverruimte heeft een passende brandblusser.

#### 11.2.2 Nutsvoorzieningen

Het gebouw waar ons kantoor gevestigd is, draagt zorg voor de nutsvoorzieningen; water, stroom, airconditioning, en internetaansluiting. Mochten deze voorzieningen falen, dan kunnen alle medewerkers thuis werken.

#### 11.2.3 Beveiliging van bekabeling

De bekabeling binnen het gebouw wordt door de beheerder van het gebouw gelegd en beheerd. De router bevindt zich in de serverruimte, zodat er niet eenvoudig een apparaat aangesloten kan worden dat al het netwerkverkeer afluistert.

#### 11.2.4 Onderhoud van apparatuur

Medewerkers dienen hun laptops en telefoons te updaten zodra de fabrikant een tussenupdate uitbrengt. De IT-admin draagt er zorg voor dat andere hardware, zoals de server, router, en access points up to date blijven en voert deze updates binnen een maand na release door. Alle apparatuur dient zoals door de fabrikant beschreven gebruikt en onderhouden te worden.

#### 11.2.5 Verwijdering van bedrijfsmiddelen

Alle documenten en informatie zijn opgeslagen in de cloud. Laptops en telefoons zijn bedoeld om ook buiten kantoor gebruikt te worden. Met fysieke documenten mag alleen op kantoor of thuis gewerkt worden, niet elders of onderweg.

#### 11.2.6 Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein

Apparatuur moet voldoende beschermd zijn buiten kantoor, zowel tegen externe factoren als weer en vervoer als tegen diefstal. Apparatuur mag buiten kantoor en thuis nooit onbeheerd achtergelaten worden, zelfs afgesloten niet.

#### 11.2.7 Veilig verwijderen of hergebruiken van apparatuur

Mediadragers kunnen op enig moment worden hergebruikt, maar het is belangrijk om dit proces goed te beheersen. Het medium zou geclassificeerde inhoud kunnen bevatten, die niet terug vorderbaar zou moeten worden gemaakt door het te overschrijven. Wanneer het overschrijven niet veilig kan worden gedaan, mag het medium niet opnieuw worden gebruikt en moet het worden vernietigd na overschrijven.

Het wissen of overschrijven vindt plaats door de IT-admin. Apparaten mogen hergebruikt worden, maar alleen als deze grondig gewist zijn door de IT-admin.

#### 11.2.8 Onbeheerde gebruikersapparatuur

Apparatuur is niet altijd in gebruik en dient dan goed beschermd te worden. Inlogsessies worden na een korte periode van inactiviteit automatisch beëindigd en personeel moet zich na sessies handmatig uitloggen. Apparatuur mag buiten kantoor en thuis nooit onbeheerd achtergelaten worden, zelfs afgesloten niet.

#### 11.2.9 Clear desk- en clear screen beleid

Bij het verlaten van het kantoor moeten alle documenten van de bureaus worden verwijderd en op een niet-zichtbare manier worden opgeslagen. Vertrouwelijke documenten moeten worden opgeslagen in vergrendelde laden of archiefkasten.

* Computers en telefoons moeten een schermbeveiliging hebben met een wachtwoord of een soortgelijke veiligheidsmaatregel (bijvoorbeeld een vingerafdruklezer). Medewerkers moeten apparaten altijd vergrendelen wanneer ze deze onbewaakt achterlaten.
* Schermen mogen geen bedrijfsinformatie bevatten (ook geen meldingen verschijnen) wanneer ze worden getoond aan mensen buiten het bedrijf, bijvoorbeeld aangesloten op een externe projector. Dit geldt ook voor virtuele bureaubladen.
* Er mag niet met gevoelige informatie gewerkt worden op een publieke locatie of in een publiek kantoor.

# Beveiliging bedrijfsvoering (A12)

### Bedieningsprocedures en verantwoordelijkheden

#### 12.1.1 Gedocumenteerde bedieningsprocedures

Op onze intranet hebben de verschillende teams pagina’s gemaakt over hun eigen processen en werkwijzen.

#### 12.1.2 Wijzigingsbeheer

Alle wijzigingen in- en binnen de organisatie die van invloed kunnen zijn op de informatiebeveiliging worden gecontroleerd en goedgekeurd door het management. Dergelijke veranderingen kunnen bijvoorbeeld het gebruik van een nieuw systeem of een verandering in een belangrijk bedrijfsproces zijn.

Wijzigingen aan het ISMS of met een risico op onderbrekingen, worden in de weekplanning besproken en gepland om impact voor klanten te beperken. Er wordt een ticket gemaakt per wijziging waarin risicobeperkende maatregelen worden benoemd.

#### 12.1.3 Capaciteitsbeheer

Onze cloudomgeving schaalt dynamisch mee qua opslag en processorkracht. Infrastructuur wordt geschaald met toekomstige groei in het achterhoofd en wordt regelmatig door [ROL] beoordeeld.

#### 12.1.4 Scheiding van ontwikkel-, test-, en productieomgevingen

Voor alle grote IT-systemen moeten tests eerder in afzonderlijke testomgevingen worden uitgevoerd en kunnen wijzigingen of tests tijdens de productie worden uitgevoerd. Ontwikkelaars hebben geen toegang tot de productieomgeving.

### Bescherming tegen malware

#### 12.2.1 Beheersmaatregelen tegen malware

Alle computers (servers, pc's en laptops) moeten zijn uitgerust met een regelmatig bijgewerkte virusscanner en een firewall. Indien mogelijk moeten gebruikers worden belet scanners, firewalls uit te schakelen of andere beveiligingswijzigingen aan te brengen.

### Back-up

#### 12.3.1 Back-up van informatie

[BEDRIJF] zorgt voor adequate back-up- en hersteldiensten om de beschikbaarheid van de service en gegevens te garanderen. De gegevens worden opgeslagen in een database en worden opgeslagen zolang de cliënt cliënt blijft van [BEDRIJF]. Er wordt dagelijks een back-up gemaakt waarmee de applicatie dagelijks tot [AANTAL] dagen in het verleden kan worden hersteld.

De back-upprocedures worden jaarlijks getest op juistheid en volledigheid van de gegevensopslag, correctheid van procedures en benodigde hersteltijd in geval van een incident.

### Verslaglegging en monitoren

#### 12.4.1 Gebeurtenissen registreren

Logboekregistratie van gebeurtenissen moet voor alle servers zijn ingeschakeld. Gebeurtenissen die moeten worden vastgelegd, omvatten mislukte inlogpogingen, upgrades van toegangsrechten, aanmaken van accounts, toegang tot logbestanden, toegang tot gevoelige informatie en alle wijzigingen / verwijderingen. [SOFTWARE] wordt gebruikt voor logboekregistratie.

#### 12.4.2 Beschermen van informatie in logbestanden

De logboeken moeten veilig worden opgeslagen, beschermd tegen manipulatie en waarschuwingen / meldingen bevatten voor onregelmatige activiteiten. De logboeken worden ten minste een jaar opgeslagen om onderzoek mogelijk te maken.

#### 12.4.3 Logbestanden van beheerders en operators

Bevoorrechte accounts zoals admin- of operatoraccounts hebben toegang tot logboeken, dus het is belangrijk om hun toegang tot de logs van hun eigen activiteit te beperken. Om de integriteit van geprivilegieerde accountlogboeken te behouden, wordt een ander logboeksysteem ingevoerd dat niet toegankelijk is voor de bevoorrechte personen.

#### 12.4.4 Kloksynchronisatie

Op alle servers moet een tijdsynchronisatieservice zijn geïnstalleerd, zodat logbestanden nauwkeurige timinginformatie bevatten. Dit wordt afgehandeld door [SYSTEEM].

### Beheersing van operationele software

#### 12.5.1 Software installeren op operationele systemen

Installatie van software op operationele systemen wordt gecontroleerd. Er is een gedocumenteerde procedure van hoe software wordt gecontroleerd vóór de installatie en wie de software installeert / bijwerkt / verwijdert en hoe. Het installeren, bijwerken of verwijderen van software zonder de impact op de operationele omgeving te beoordelen, kan negatieve gevolgen hebben.

Serverinstallatie is zoveel mogelijk geautomatiseerd om gebruikersfouten te minimaliseren.

**Belangrijk:** software-updates worden gedaan op [TIJD\_PERIODE].

### Beheer van technische kwetsbaarheden

#### 12.6.1 Beheer van technische kwetsbaarheden

Ten minste jaarlijks vindt een architectuurreview plaats, waarbij alle versies van belangrijke softwarecomponenten worden geïdentificeerd. Er wordt gevalideerd dat alle versies nog steeds worden ondersteund en dat dit de meest recente of de tweede meest recente versie is.

#### 12.6.2 Beperking op het installeren van software

[BEDRIJF] beperkt de toegang van gebruikers niet. Ze kunnen zelf software installeren die relevant is voor hun werkzaamheden. Software die niet relevant is voor werkzaamheden, bijvoorbeeld videogames en privé social media apps mag niet geïnstalleerd worden.

Alleen software van reputabele bedrijven mag geïnstalleerd worden, en de bron dient altijd geverifieerd te worden voor de installatie. Deze regels worden ook gedekt tijdens de awareness training.

#### 12.7.1 Beheersmaatregelen betreffende audits van informatiesystemen

[BEDRIJF] staat audits van klanten in contractueel overeengekomen vorm toe. Audits kunnen diepe toegang tot veel informatie vereisen, wat de dagelijkse activiteiten van het personeel niet mag verstoren. Om een vlotte audit te garanderen:

* Alle auditors moeten een duidelijk auditplan hebben;
* De audit plan moet goedgekeurd worden door de CEO;
* Het auditplan moet minimaal twee weken van tevoren worden meegedeeld;
* Elke auditee krijgt vooraf inzicht in het onderwerp van elk gesprek.

.

# Communicatiebeveiliging (A13)

### Beheer van netwerkbeveiliging

#### 13.1.1 Beheersmaatregelen voor netwerken

Alle netwerken moeten beveiligingsmaatregelen hebben om beschermd te zijn tegen bemoeiing en afluisteren. De router bevindt zich in een afgesloten ruimte, en de access points hangen op een moeilijk bereikbaar plek. Er zijn firewalls op beide kantoornetwerken, op gateways in de cloud, en alle laptops van medewerkers. De firewalls worden geconfigureerd en beheerd door de IT-admin, en jaarlijks gecontroleerd door de Security Officer.

#### 13.1.2 Beveiliging van netwerkdiensten

De wifinetwerken zijn beveiligd met een wachtwoord en een firewall. De IT-admin configureert de firewall op basis van de geïdentificeerde risico’s en best practices in de markt. De volgende firewall regels zijn ingesteld:

* [REGEL 1]
* [REGEL 2]
* Etc.

#### 13.1.3 Scheiding in netwerken

[BEDRIJF] heeft een gescheiden gastnetwerk, namelijk [SSID NETWERK]. Gasten en andere bezoekers mogen alleen met dit netwerk verbinding maken. Medewerkers mogen alleen van het hoofdnetwerk [SSID NETWERK] gebruik maken. De twee netwerken zijn gescheiden. De wachtwoorden worden jaarlijks gewijzigd.

[BIJ NETWERKEN IN DE CLOUD]

[BEDRIJF] heeft de volgende virtuele netwerken in de cloud:

* Netwerk 1
* Netwerk 2

Een schematische weergaven van de netwerkarchitectuur is hier te vinden: [LINK DIAGRAM].

### Informatietransport

#### 13.2.1 Beleid en procedures voor informatietransport

Aangezien iedereen op dezelfde locatie werkt, is er geen behoefte aan interne fysieke transportprocedures. Informatie wordt zo veel mogelijk elektronisch overgedragen, bijvoorbeeld via [SOFTWARE].

#### 13.2.2 Overeenkomsten over informatietransport

Niet van toepassing

#### 13.2.3 Elektronische berichten

De volgende manieren van berichten uitwisseling is toegestaan bij [BEDRIJF]:

1. Type A
2. B
3. C
4. n

#### 13.2.4 Vertrouwelijkheid- of geheimhoudingsovereenkomst

Medewerkers van [BEDRIJF] zijn contractueel gebonden aan geheimhouding. Dit geldt ook voor part-time medewerkers, stagiairs, en freelancers.

# Acquisitie, ontwikkeling en onderhoud van informatiesystemen (A14)

### Beveiligingseisen voor informatiesystemen

#### 14.1.1 Analyse en specificatie van informatiebeveiligingseisen

Als er software wordt ontwikkeld voor de websites (nieuwe formulieren, widgets) dan wordt vooraf een ontwerp gedaan dat in lijn in met OWASP en AVG. Concreet betekent dit het afschermen en veilig sturen voor informatie, validatie van input, niet meer persoonsgegevens verzamelen dan nodig is. Voor ontwikkeling wordt een projectplan gemaakt, hierin worden ook de beveiligingseisen opgenomen.

#### 14.1.2 Toepassingsdiensten op openbare netwerken beveiligen

Alle systemen die communiceren via internet of openbare netwerken, moeten versleutelde beveiligde verbindingen gebruiken voor gegevensoverdracht, omdat het internetprotocol zelf geen bescherming biedt tegen afluisteren of tussenkomst. Aanbevolen technologie omvat SSL en gerelateerde protocollen zoals https en sftp.

#### 14.1.3 Transacties van toepassingsdiensten beschermen

Bij functies waarbij sprake is van aankopen, transacties of betalingen, wordt gezorgd voor goede beveiliging. Dit kan door gebruik te maken van standaard-diensten zoals Eventbrite of erkende payment service providers.

### Beveiliging in ontwikkelings- en ondersteunende processen

#### 14.2.1 Beleid voor beveiligd ontwikkelen

Er is een standaard / richtlijn voor veilige applicatie-ontwikkeling, zodat elke ontwikkelaar het belang van beveiliging kent en de OWASP top 10-kwetsbaarheden begrijpt en hoe deze te voorkomen. Ontwikkelaars ontvangen regelmatig beveiligingstraining (minstens één keer per jaar).

Systeemeigenaars, ontwerpers en beheerders worden geïnstrueerd over het belang van privacy en beveiliging door ontwerp. Als onderdeel van de instructie moeten ze leren dat ze verantwoordelijk zijn voor de volgende aspecten:

Persoonsgegevens mogen niet worden verzameld wanneer ze niet nodig zijn, zonder reden of toestemming. Persoonsgegevens moeten veilig worden opgeslagen en beschermd worden, bijvoorbeeld gebruik van codering of hashen. Persoonsgegevens moeten na gebruik actief worden verwijderd, aangezien het niet is toegestaan ze langer dan noodzakelijk op te slaan.

#### 14.2.2 Procedures voor wijzigingsbeheer met betrekking tot systemen

Het ticketingsysteem [TICKETING\_SYSTEEM] wordt bij ons gebruikt om alle wijzigingen te documenteren. Changes worden gereviewd door [ROL] voordat ze geïmplementeerd worden, en moeten aan de eisen voldoen die we in onze development policy beschreven hebben.

#### 14.2.3 Technische beoordeling van toepassingen na wijzigingen bedieningsplatform

Na een wijziging worden operationele systemen beoordeeld op hun prestaties en beveiliging. De wijziging kan het systeem of de algehele informatiebeveiliging en / of -prestaties negatief hebben beïnvloed.

#### 14.2.4 Beperkingen op wijzigingen aan softwarepakketten

Softwarepakketten vereisen af en toe updates, die klein of groot kunnen zijn. Er is een procedure voor het updaten van de software: de hoofdversie is vastgezet en een kleine versie wordt geaccepteerd zodra deze beschikbaar is.

#### 14.2.5 Principes voor engineering van beveiligde systemen

Alle medewerkers worden minstens jaarlijks getraind in de ontwikkeling van veilige software. De basis voor de training is de OWASP top 10.

#### 14.2.6 Beveiligde ontwikkelomgeving

We hebben een secure development beleid dat gebaseerd is op OWASP. Dit beleid is te vinden op Confuence. [LINK] Het beleid is gebaseerd op de OWASP Top 10 Web App risico’s. Software wordt lokaal ontwikkeld, en alleen lead developers mogen pull requests naar productie accepteren. Dezelfde veiligheidsmaatregelen zijn getroffen voor productie en acceptatie.

#### 14.2.7 Uitbestede softwareontwikkeling

[BEDRIJF] doet niet aan de uitbesteding van softwareontwikkeling.

#### 14.2.8 Testen van systeembeveiliging

Beveiligingstests worden regelmatig uitgevoerd voor alle systemen als onderdeel van het ontwikkelingsproces. Ten minste elk jaar wordt een onafhankelijk, extern beveiligingsbedrijf gevraagd om een PEN-test uit te voeren (penetratietest) om te testen of IT-systemen duidelijke tekortkomingen vertonen. De bevindingen worden gerapporteerd aan het management en gebruikt voor het versterken van zowel de systemen en ontwikkelings- en testprocessen.

#### 14.2.9 Systeemacceptatietests

Tijdens de ontwikkeling wordt de veiligheid van het nieuwe / bijgewerkte systeem ook getest tijdens reguliere tests.

### Testgegevens

#### 14.3.1 Bescherming van testgegevens

[ORGANISATIE] beveiligt acceptatieomgevingen net zo goed als productieomgevingen. In de acceptatieomgevingen wordt minimaal vertrouwelijke informatie gebruikt, bij voorkeur alleen persoonsgegevens van bij project betrokken personen. In acceptance wordt geanonimiseerde productiedata gebruikt. In de testomgeving wordt nooit productiedata gebruikt.

# Leveranciersrelaties (A15)

### Informatiebeveiliging in leveranciersrelaties

#### 15.1.1 Informatiebeveiligingsbeleid voor leveranciersrelaties

We hebben een register van leveranciers, dat jaarlijks gecontroleerd wordt door de security officer. Van elke leverancier wordt bijgehouden welke afspraken er zijn, of er een verwerkersovereenkomst is, en wat het niveau van dienstverlening is geweest het afgelopen jaar. Als een leverancier ondermaats presteert, wordt er door de directie een gesprek met deze partij gevoerd, of wordt de dienstverlening opgezegd.

#### 15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

Het is naar Nederlands recht verplicht dat een verwerkingsovereenkomst wordt ondertekend met elke leverancier die toegang heeft tot persoonlijke gegevens. [ROL] moet de relevante wetgeving en publicaties van de Autoriteit Persoonsgegevens lezen, een templateovereenkomst maken die moet worden gebruikt en ervoor zorgen dat overeenkomsten worden gesloten met elke bestaande en nieuwe leverancier.

**Belangrijk:** er wordt een lijst bijgehouden van alle locaties waar hun assets worden verwerkt, verzonden, opgeslagen of geopend. Het maakt deel uit van het assetoverzicht. Het wordt op verzoek naar klanten gestuurd

Deze lijst wordt minimaal één keer per jaar bijgewerkt.

#### 15.1.3 Toeleveringsketen van informatie- en communicatietechnologie

In de contracten met leveranciers wordt overeengekomen dat de leverancier volledig verantwoordelijke is voor enige subleveranciers die zij inschakelen. Van leveranciers van kritieke software eisen wij een ISO27001 certificering.

### Beheer van dienstverlening van leveranciers

#### 15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

We reviewen de dienstverlening van leveranciers jaarlijks, en houden dit bij in het leveranciersregister. Voorbeelden van eisen die aan leveranciers gesteld worden zijn Uptime, incident response tijd, en mate waarin aan contractuele afspraken voldaan wordt.

#### 15.2.2 Beheer van veranderingen in dienstverlening van leveranciers

Met leveranciers is contractueel afgesproken dat zij significante wijzigingen in hun dienstverlening aan ons melden alvorens deze door te voeren. In zulke gevallen overlegt de Security Officer met de directie of de dienstverlening doorgezet of stopgezet wordt.

# Beheer van informatiebeveiligingsincidenten (A16)

### Beheer van informatiebeveiligingsincidenten en -verbeteringen

#### 16.1.1 Verantwoordelijkheden en procedures

Een datalek is elke gebeurtenis waarbij persoonlijke gegevens mogelijk verloren gaan of worden gelekt naar de buitenwereld. Een dergelijk incident moet worden onderzocht en mogelijk worden gemeld aan de Autoriteit Persoonsgegevens (AP) en de betrokkenen die worden getroffen.

 Andere personeelsleden moeten de verantwoordelijke persoon op de hoogte stellen van een mogelijk datalek en onderzoek ondersteunen.

#### 16.1.2 Rapportage van informatiebeveiligingsgebeurtenissen



Onze definities zijn als volgt:

**Gebeurtenis:** Een concreet event (met tijd en datum) dat te maken heeft met informatiebeveiliging.

**Incident:** Een gebeurtenis met een negatieve impact op de B, I, en/of V van een informatie-asset.

**Kwetsbaarheid:** Zwakke plek in de informatiebeveiliging die zou kunnen leiden tot een incident.

Als werknemers gegronde redenen hebben om aan te nemen dat er zich een incident heeft voorgedaan, moeten ze het incident **onmiddellijk** melden bij de IB-officer. In veel gevallen is het bedrijf verplicht om incidenten onmiddellijk te onderzoeken en te melden aan klanten of de autoriteiten. Het bedrijf kan dit alleen doen als het personeel alert is. Wanneer de IB-officer niet kan worden bereikt, rapporteer het incident aan andere InfoSec teamleden of aan het management. In geval van twijfel moeten medewerkers het incident altijd melden.

#### 16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Een kwetsbaarheid moet ook worden gemeld, maar is minder urgent. Ze moeten dezelfde dag of de volgende dag via e-mail aan de IB-officer of aan het InfoSec-team worden gemeld. Deze zullen de kwetsbaarheid analyseren en oplossen. Als werknemers niet zeker weten of iets een kwetsbaarheid is, kunnen ze het nog steeds melden als een potentiële kwetsbaarheid en zal het Infosec-team bepalen of het een kwetsbaarheid is en welke actie nodig is.

#### 16.1.4 Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen

De persoon die verantwoordelijk is voor deze control moet de officiële AP-richtlijnen bestuderen en de rapportage uitvoeren.

#### 16.1.5 Respons op informatiebeveiligingsincidenten

Zie [appendix 0](#_Bijlage_0:_Procedure) voor de volledige procedure.

#### 16.1.6 Lering uit informatiebeveiligingsincidenten

Alle grote incidenten worden besproken door het IB-team. Zij zullen de achterliggende oorzaak bepalen en extra maatregelen voorstellen.

#### 16.1.7 Verzamelen van bewijsmateriaal

Technisch personeel slaat een beschrijving op van beveiligingsincidenten (logs, screenshots). Voor grote incidenten worden logbestanden veilig opgeslagen voor latere analyse.

# Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer (A17)

### Informatiebeveiligingscontinuïteit

#### 17.1.1 Informatiebeveiligingscontinuïteit plannen

Belangrijke continuïteitsrisico's worden beheerd door het gebruik van een cloud-based architectuur. Back-ups worden buiten [NORMALE\_OPSLAG\_LOCATIE] geplaatst in het geval van een [NORMALE\_OPSLAG\_LOCATIE] onderbreking. Het gebouw heeft een evacuatieplan is een geval van brand.

De volledige lijst van continuïteitsrisico’s en maatregelen is te vinden in het BCP plan. [LINK]

#### 17.1.2 Informatiebeveiligingscontinuïteit implementeren

In het BCP plan zijn per scenario maatregelen opgenomen. Deze maatregelen zijn opgesteld na de risicoanalyse, en vervolgens door de Security Officer geïmplementeerd.

#### 17.1.3 Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren

Er wordt jaarlijks een controle gedaan of de BCP maatregelen passend zijn en werken. Niet-passende maatregelen, bijvoorbeeld omdat een risicoscenario niet meer van toepassing is, worden opgeschort.

De jaarlijkse controle bestaat uit een praktische test, waarvan verslag gelegd wordt door de Security Officer. Zo hebben wij bijvoorbeeld een jaarlijkse thuiswerkdag, en wordt het terugzetten van back-ups getest tijdens de jaarlijkse restore dag.

### Redundante componenten

#### 17.2.1 Beschikbaarheid van informatieverwerkende faciliteiten

Met onze cloudleverancier [NAAM] hebben wij contractueel afgesproken dat de uptime 99.95% moet zijn, met maximale onderbrekingen van 30 minuten per keer.

Met onze emailprovider [NAAM] hebben wij contractueel afgesproken dat de uptime 99% moet zijn, met maximale onderbrekingen van 1 uur per keer.

Wij bieden onze klanten een uptime van 98% aan. Dit houden wij in de gaten met [SOFTWARE], die een slackbericht stuurt naar [PERSOON] als de service down is.

# Naleving (A18)

### Naleving van wettelijke en contractuele eisen

#### 18.1.1 Vastleggen van toepasselijke wetgeving en contractuele eisen

In het document Wet- en regelgeving [LINK] hebben wij een overzicht van alle wetgeving, regelgeving, en contractuele eisen die invloed hebben op ons ISMS.

Als we op de een of andere manier een claim van een derde ontvangen met betrekking tot de gegevens van- of samenwerking met een klant, zullen we die klant binnen 30 dagen vanaf de datum waarop we de claim wisten op de hoogte brengen. [BEDRIJF] heeft een aansprakelijkheidsverzekering bij [VERZEKERAAR].

#### 18.1.2 Intellectuele eigendomsrechten

[BEDRIJF] respecteert Intellectueel Eigendom. Medewerkers dienen te controleren of een asset gebruikt kan worden, voor zij het gebruiken. Illegale software, of software zonder licentie mag niet gebruikt worden.

#### 18.1.3 Beschermen van registraties

De documenten opgeslagen in het cloudsysteem [CLOUDSYSTEEM] heeft een automatische back-up termijn van [AANTAL] dagen. Alleen beheerders kunnen bestanden echt verwijderen voor deze termijn verstreken is.

Logbestanden, opgeslagen in [SOFTWARE], zijn alleen voor [ROL] toegankelijk en kunnen niet handmatig gewist worden.

#### 18.1.4 Privacy en bescherming van persoonsgegevens

Persoonlijk identificeerbare informatie (PII), ook wel Persoonsgegevens genoemd, dient met de grootst mogelijke zorgvuldigheid te worden behandeld. Voorbeelden van PII zijn burgerservicenummers, e-mailadressen en namen. Dit leidt tot de volgende regels:

* Beperk de distributie en opslag van PII zoveel mogelijk
* Als je PII verzendt, moet je de ontvanger op de hoogte stellen van het beoogde gebruik. Als je bijvoorbeeld in HR werkt, moet je bij het verzenden van een cv van een mogelijke nieuwe aanwerving expliciet vermelden dat de persoon het kan gebruiken voor het sollicitatiegesprek en het daarna moet verwijderen. Geef aan dat ze het cv niet kunnen doorsturen en je om meer informatie moeten vragen als ze het nodig hebben.
* Gebruik alleen vertrouwde systemen voor de distributie en opslag van PII.

Indien contractueel overeengekomen, worden klantgegevens opgeslagen in een aparte database.

Bij [BEDRIJF] hebben we een [DPO of PRIVACY OFFICER]. Deze ziet er op toe dat wij aan alle wettelijke eisen voldoen die voortkomen uit de AVG, zoals een up-to-date verwerkingsregister, privacystatement en doen van een DPIA. Een DPIA wordt uitgevoerd wanneer er sprake is van verwerking van bijzondere persoonsgegevens of grote verandering van onze werkwijze.

#### 18.1.5 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

In sommige landen is het gebruik van cryptografie aan beperkingen onderhevig. [ORGANISATIE] [ROL] controleert welke regels van toepassing zijn voordat ze buiten de EU reizen. Indien nodig wordt een schoon leeg apparaat meegenomen in plaats van normale laptops.

### Informatiebeveiligingsbeoordelingen

#### 18.2.1 Onafhankelijke beoordeling van informatiebeveiliging

Er wordt jaarlijks een interne ISMS audit gedaan door [ROL/EXTERNE PARTIJ]. Zo dragen wij er zorg voor dat de interne audit onafhankelijk plaatsvindt. De resultaten worden direct na de interne audit met de directie besproken, zodat verbeterpunten z.s.m. opgepakt kunnen worden.

#### 18.2.2 Naleving van beveiligingsbeleid en -normen

#### Met al deze beleidsregels, normen en procedures op het gebied van beveiliging is het voor managers belangrijk om regelmatig te beoordelen of de activiteiten en/of processen waarvoor ze verantwoordelijk zijn volledig compliant zijn. Om dit correct te doen, moeten ze precies weten aan welke regels en vereisten ze moeten voldoen en moeten ze dit controleren.

#### 18.2.3 Beoordeling van technische naleving

Informatiesystemen worden ook regelmatig beoordeeld op naleving. Kwetsbaarheidstests zoals penetratietests worden jaarlijks gedaan, net als pre-audits.

Klanten, zoals [KLANTEN] kunnen verzoeken om (een partij in te huren om) een PEN-test uit te voeren op onderdelen van ons systeem. Deze test mag alleen worden uitgevoerd met onze uitdrukkelijke schriftelijke toestemming en op door ons aangewezen / goedgekeurde delen van het systeem.

# Bijlage: Procedure meldplicht datalekken

[BEDRIJF] hanteert de volgende procedure meldplicht datalekken. Deze is oorspronkelijk gebaseerd op de richtsnoeren van de autoriteit persoonsgegevens en aangepast op basis van de AVG.

#### Melding aan securityteam

Iedereen binnen [BEDRIJF] is geïnstrueerd om mogelijke lekken, security-incidenten en zelfs vragen te stellen aan het security-team.

Leveranciers zijn door middel van bewerkersovereenkomsten ook op de hoogte gesteld van hun plicht om datalekken te melden via [SECURITY\_MAILADRES].

In elke training worden de contactgegevens genoemd.

#### Definities

[BEDRIJF] hanteert de volgende definities:

Een **(beveiligings-)incident** is een concrete gebeurtenis waarbij de beschikbaarheid, confidentialiteit of integriteit van een informatie-asset is geschonden.

Een **datalek** is een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of de ongeoorloofde verstrekking van of de ongeoorloofde toegang tot doorgezonden, opgeslagen of anderszins verwerkte gegevens.

Een **persoonsgegeven** is elk gegeven dat herleidbaar is tot een natuurlijk persoon. Denk aan email, telefoonnummer, voornaam\_achternaam, huisadres, kenteken, IP-nummer, bankrekeningnummer, MAC-adres, foto's met gezichten erop, inkomen, geboortedatum. Niet persoongegevens zijn gemiddeldes over grote groepen.

#### Afhandeling van meldingen mogelijke datalekken

Het information securityteam is verantwoordelijk voor de procedure meldplicht datalekken. Elk beveiligingsincident moet worden gemeld bij het securityteam en wordt door het team gelogd en bestudeerd.

Voor elk datalek wordt deze procedure doorlopen:

1. Het team bestudeert het incident en bepaalt wat er wanneer en waar is gebeurd en welke apparatuur en partijen hierbij betrokken zijn geweest

2. Het team neemt indien relevant direct actie om het lek te dichten of te stoppen, of spoort IT-betrokkenen aan om dit direct te doen.

3. Het team bepaalt welke persoonsgegevens van hoeveel en welke personen er betrokken zijn. Als uitkomst hiervan wordt het aantal personen vastgelegd, welke soorten gegevens en of er sprake is van bijzondere gegevens.

4. Het team bepaalt wie de verantwoordelijke voor de gegevens is. Dit wordt bepaald door na te gaan hoe de gegevens zijn verkregen en door bestudering van alle verwerkersovereenkomsten waaronder de gegevens zijn doorgegeven.

5. Het team bepaalt uitsluitbaarheid: of het redelijkerwijs uit te sluiten is dat persoonsgegevens onrechtmatig zijn verwerkt. Dit is bijvoorbeeld het geval bij diefstal van een laptop die voorzien is van sterke encryptie.

6a. Als [BEDRIJF] geen verantwoordelijke is maar verwerker, wordt er melding gedaan conform de contactgegevens in verwerkersovereenkomst. Indien dit niet duidelijk is of niet uitvoerbaar, wordt contact opgenomen via telefoonnummer op website van partij. Het streven is om dit te doen binnen 8 kantooruren na ontdekking incident (of conform termijn in bewerkersovereenkomst).

6b. Als er sprake is van een datalek en [BEDRIJF] verantwoordelijke is, dan doet het security-team het volgende:

* Op de hoogte stellen directie van [BEDRIJF] zodat zij input kunnen geven over de inschatting van kan op ernstige nadelige gevolgen. De directie overlegt indien zij dat wensen met externe experts.
* Afronden onderzoek en goed vastleggen uitkomsten in een apart incidentrapport
* Incident melden via het webformulier bij de Autoriteit Persoonsgegevens. Dit moet indien mogelijk niet later dan 72 uur na ontdekking.
* Het security-team schat in of het melden aan betrokkenen mogelijk is en of een melding eventueel nadelige gevolgen heeft voor de betrokken persoon. NB: als er sprake is van goede encryptie en de kans op gevolgen voor betrokken hierdoor minimaal is, hoeft melding niet.
* Als het mogelijk is om te melden, dit geen nadelen heeft voor betrokkenen en er geen sprake is van goede encryptie, worden het datalek gemeld aan betrokkenen.

Alle besluiten over bijvoorbeeld ernst, uitsluitbaarheid, wel/niet melden worden vastgelegd in een verslag over het incident.

De gegevens van het incident en de melding worden bewaard als onderdeel van het ISMS door het information security team. [BEDRIJF] bewaart incidenten in principe drie jaar om het ISMS te kunnen blijven evalueren en verbeteren.

*Klanten kunnen, op verzoek, een kopie van onze datalekprocedure ontvangen.*

# Bijlage: bezoekersregistratie

De volgende regels gelden voor het [BEDRIJF] hoofdgebouw in [STAD].

Op werkdagen tussen [OPEN] en [SLUIT] is er een receptionist(e) aanwezig bij de ingang. De receptionist vraagt iedereen die aanbelt of deze bezoeker is of externe medewerker.

Regels bezoekers:

* De bezoeker moet zich inschrijven op de lijst en moet wachten bij de receptie. De receptionist belt de contactpersoon. Deze haalt de bezoeker op.
* De contactpersoon is verantwoordelijk voor de bezoeker en begeleidt deze in het pand. Bezoekers mogen niet zelf rondlopen.
* Als de receptie niet bemand is en een medewerker laat iemand binnen, dan is deze medewerker er verantwoordelijk voor dat de bezoeker niet vrij rondloopt. Vraag de bezoeker met wie de afspraak is, en breng de bezoeker naar deze persoon toe.

Regels externe medewerkers:

* Externe medewerkers die toestemming hebben van hun leidinggevende (directie of afdelingsmanager) mogen zelfstandig rondlopen. Hiervoor ligt een lijst van bekende externe medewerkers bij receptie.
* Indien externe medewerker niet bekend is, wordt de leidinggevende gebeld. Deze haalt de externe medewerker op en zet hem of haar op de lijst.

Aannemen poststukken en pakketten

* De receptioniste neemt post en pakketten aan als deze aan [BEDRIJF] is geadresseerd.
* Alle poststukken worden gestempeld met datum van ontvangst. De receptioniste brengt de stukken naar de juiste persoon of afdeling.
* Voor alle aangetekende post die ontvangen wordt, wordt de datum van ontvangst in een schrift genoteerd.