Informatie-beveiliging: Beleid en doelstellingen

Dagtekening document: 28 jun 2024

Inhoudsopgave

1. Inleiding

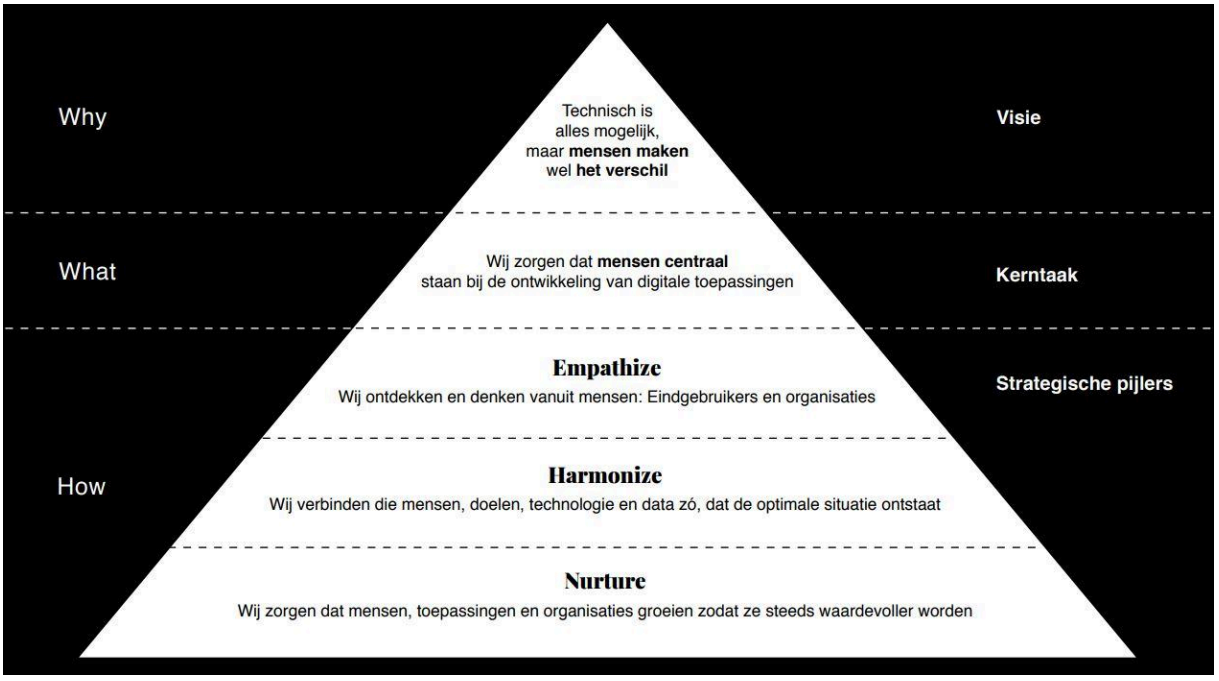
1.1 Achtergrond

Dit document beschrijft het beleid van theFactor.e voor de beveiliging van informatie. Het beleid is tot stand gekomen door het uitvoeren van een risicoanalyse en nulmeting informatiebeveiliging. Bepaald is in hoeverre de bedrijfsprocessen van theFactor.e afhankelijk zijn van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie. Ook zijn relevante bedreigingen en kwetsbaarheden in kaart gebracht. Er zijn vervolgens passende maatregelen geselecteerd. De maatregelen zijn getoetst. Het beleid is gebaseerd op de eisen die de Code voor Informatiebeveiliging (ISO 27001:2022) hieraan stelt.

1.2 Bedrijfscontext

theFactor.e is een full service internetbureau. We helpen klanten met het formuleren van hun online strategie en hun online doelen. We bedenken, bouwen en beheren digitale toepassingen.

Waarde propositie theFactor.e



De dienstverlening van theFactor.e bestaat uit de volgende diensten :

- online strategie
- experience design
- development & beheer
- devops & hosting

- data & customer intelligence
- research
- detachering

Dit doen we voor middelgrote klanten zowel in de zorg, het onderwijs en de financiële sector. theFactor.e is een belangrijke (onder)leverancier voor onze klanten. Onze klanten zijn afhankelijk van de maatregelen die theFactor.e treft. Onze klanten komen uit zeer verschillende industrieën, met in vele gevallen ook gevoelige data. Onze klanten, en op hun beurt de klanten van onze klanten, mogen van ons bedrijf verwachten dat we zorgvuldig omgaan met deze data.

Onze organisatie en onze informatievoorziening wordt blootgesteld aan een aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren. Uit inschatting en de uitgevoerde risicoanalyse kwam naar voren dat vooral de beheersing van informatie in de volgende bedrijfsprocessen belangrijk is:

Software & Ontwikkeling (in beheer en project)
Software Hosting
Financiële Administratie
HR Administratie
Sales
Inkoop

Omdat Hosting en Ontwikkeling op klantbasis uitgevoerd worden moet met een goede inschatting per project gewerkt worden en een goede minimale norm vastgehouden worden om garanties te kunnen bieden over de hele bedrijfsvoering.

1.3 Bedrijfsdoelstellingen

De eindgebruiker wordt door theFactor.e centraal gesteld. We bouwen, ontwerpen, verbeteren altijd voor eindgebruikers. theFactor.e vindt het belangrijk dat we verantwoordelijk omgaan met de data die wij in dit proces verwerken, privacy en beveiliging staan daarom hoog in het vaandel.

We werken voor klanten die deze eindgebruiker veelal ook centraal stelt. Een subdoelstelling van dit beleid is derhalve om onze klanten te ontzorgen op het vlak van informatiebeveiliging binnen onze dienstverlening zoals deze in paragraaf 1.2 verwoord is.

Verder constateren we dat de wet- en regelgeving rondom informatiebeveiliging, die als einddoel heeft om de eindgebruiker te beschermen, zich continu ontwikkelt. We houden ons op de hoogte, groeien mee met nieuwe ontwikkelingen en informeren onze stakeholders pro-actief waar dit meerwaarde heeft. Op deze wijze staan we bekend als expert, voldoen we aan regelgeving, bedienen we onze klanten optimaal en is de eindgebruiker zo goed mogelijk beschermd.

Als laatste is het belangrijk dat onze medewerkers bewust zijn van het *Informatiebeveiligingsbeleid,* daarnaar handelen en voldoende assistentie hebben daar waar het om informatiebeveiliging gaat. Bewustwording en training staan hoog op de agenda.

theFactor.e communiceert informatie over incidenten en awareness zaken middels centrale interne communicatiemiddelen, trainingstools en kennis-events op regelmatige basis.

Daarom streven we met ons informatiebeveiligingsbeleid het volgende na:

1. **Klanten**: We willen een strategisch partner op niveau zijn voor onze klanten, daarvoor:
    a. hebben we competent personeel dat kan adviseren op dit gebied
    b. we willen onze klanten actief kunnen ontzorgen
    c. willen we ons houden aan onze afspraken en contracten met de klant
2. **Interne Organisatie**: We willen als professionele organisatie verantwoord omgaan met data, daarom:
    a. willen we dat personeel goed op de hoogte is op het gebied van security & privacy en het goed toepassen in hun werk
    b. willen we intern correct omgaan met de gegevens van de klant, TFE en haar medewerkers
    c. willen we de risico's op schade en de continuïteit van TFE beperken
3. **Markt**: Op het gebied van ISMS willen we goed bekend staan, daarom:
    a. willen we bekend staan als organisatie die verantwoord omgaat met security & privacy
    b. willen we ons houden aan wet- & regelgeving
    c. willen we het risico op schade en naamsverlies beperken

1.4 Definitie en doelstelling van informatiebeveiliging

Informatiebeveiliging is het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen. Deze definitie bevat drie belangrijke elementen.

Informatiebeveiliging omvat een samenhangend stelsel van maatregelen. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan. Daarnaast heeft stelsel van beveiligingsmaatregelen tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd.

Tot slot is informatiebeveiliging gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van risico's, kosten en baten.

Informatiebeveiliging richt zich op de *beschikbaarheid*, *integriteit* en *vertrouwelijkheid* van informatie. Beschikbaar wil zeggen dat geautoriseerde gebruikers op het juiste moment en vooral tijdig toegang hebben tot de informatie die ze nodig hebben. Integer betekent dat de informatie juist en volledig is. Vertrouwelijk tot slot wil zeggen dat informatie alleen toegankelijk is voor degene die hiertoe is gerechtigd. Het beleid wordt binnen theFactor.e uitgewerkt in richtlijnen en procedures.

1.5 Reikwijdte/Scope

Het informatiebeveiligingsbeleid is van toepassing op de gehele organisatie, zowel op de locatie Friesestraatweg 215a als op een eventuele remote- of thuiswerkplek. De concrete aspecten die van toepassing zijn op een remote- of thuiswerkplek zijn opgenomen in de personeelsgids. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van theFactor.e met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel, op personeel dat door derden wordt ingezet om diensten te verlenen aan onze organisatie en op onze leveranciers.

1.6 Betrokken partijen

De betrokken partijen zijn opgenomen in de stakeholdermap.

1.7 Leeswijzer

In hoofdstuk 2 zijn de uitgangspunten vastgelegd die worden gehanteerd bij de toepassing van informatiebeveiliging binnen theFactor.e. In hoofdstuk 3 wordt aandacht besteed aan het beleidsproces voor informatiebeveiliging. Hoofdstuk 4 beschrijft de organisatie van informatiebeveiliging.

2. Strategie voor informatiebeveiliging

2.1 Ambitie

Informatie komt in veel vormen voor (geschreven op papier, elektronisch opgeslagen, per post of via elektronische media verzonden of in gesproken vorm). Informatiebeveiliging binnen de theFactor.e organisatie richt zich in toenemende mate op de beveiliging van elektronische gegevens en informatiesystemen. Echter, informatie is een bedrijfsmiddel dat net als andere belangrijke bedrijfsmiddelen van waarde is voor theFactor.e en dat ongeacht de gegevensdrager, voortdurend op een passende manier beveiligd dient te zijn.

theFactor.e kiest ervoor om voor informatiebeveiligingsrisico's een zogenaamd basis beveiligingsniveau te implementeren die in afstemming met de klant wordt toegepast of aangepast.

Denk hierbij bijvoorbeeld aan risico's die worden veroorzaakt door calamiteiten en storingen van belangrijke informatiesystemen. Daarnaast bepaalt het management welke (aanvullende) risico's zij, in het licht van de doelstellingen, bereid zijn te lopen. Hiertoe worden jaarlijks onder meer voor de meest kritische processen, bij belangrijke wijzigingen in de strategie, processen en/of systemen risicoanalyses uitgevoerd. Informatiebeveiliging is geen doel op zich maar dient een integraal onderdeel van de bedrijfsprocessen en informatievoorziening van theFactor.e te zijn.

theFactor.e heeft tot slot de ambitie om een proces van informatiebeveiliging voor informatiebeveiliging in te richten waarmee de geïdentificeerde risico's aantoonbaar worden beheerst, onderhouden en het niveau van informatiebeveiliging continu wordt verbeterd. Dit moet blijvend resulteren in certificering op basis van ISO27001.

2.2 Uitgangspunten

theFactor.e hanteert een aantal strategische uitgangspunten ten aanzien van informatiebeveiliging. Een strategisch uitgangspunt is een criterium waaraan de richtlijnen en maatregelen op het gebied van informatiebeveiliging binnen theFactor.e moet voldoen. De strategische uitgangspunten hebben betrekking op de aandachtsgebieden organisatie, proces, mens en techniek en zijn enerzijds gebaseerd op het beleid van theFactor.e en anderzijds op 'best practices'. theFactor.e hanteert de volgende strategische uitgangspunten ten aanzien van informatiebeveiliging:

a. theFactor.e streeft ernaar aantoonbaar te voldoen aan de norm ISO 27001.
b. theFactor.e voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden onder andere genoemd:
    - Algemene Verordening Persoonsgegevens (AVG)
c. Het informatiebeveiligingsbeleid is risico-gedreven, d.w.z. dat risico's worden geïdentificeerd en maatregelen worden getroffen de risico's te mitigeren.
d. Beveiliging van informatie is een onderdeel van de integrale (management)verantwoordelijkheid. Binnen theFactor.e zijn hiertoe verantwoordelijkheden voor informatiebeveiliging toegewezen en vastgelegd.
e. Wanneer theFactor.e samenwerkingsverbanden aangaat met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed

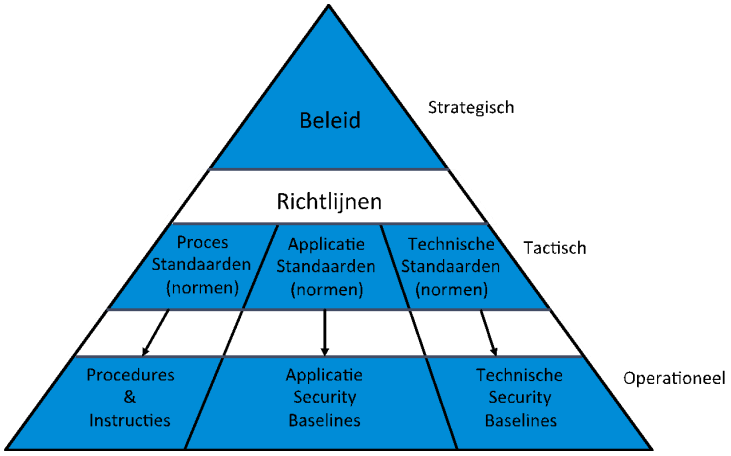
aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien.

f. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van theFactor.e zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
g. Bij de aanname, tijdens het dienstverband en in het geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
h. theFactor.e voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.
i. theFactor.e beschikt over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
j. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan theFactor.e een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de arbeidsvoorwaarden en -reglementen.
k. theFactor.e heeft maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
l. theFactor.e heeft maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, etc.) vormen hierbij een belangrijk onderdeel.
m. theFactor.e heeft maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
n. Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
o. theFactor.e heeft adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
p. Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen theFactor.e door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
q. theFactor.e beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.
r. theFactor.e controleert en evalueert periodiek het beleid en de beleidsdoelstellingen

3. Proces voor informatiebeveiliging

3.1 Raamwerk informatiebeveiliging

theFactor.e geeft op drie niveaus invulling aan informatiebeveiliging. Het raamwerk voor informatiebeveiliging is als volgt opgebouwd:



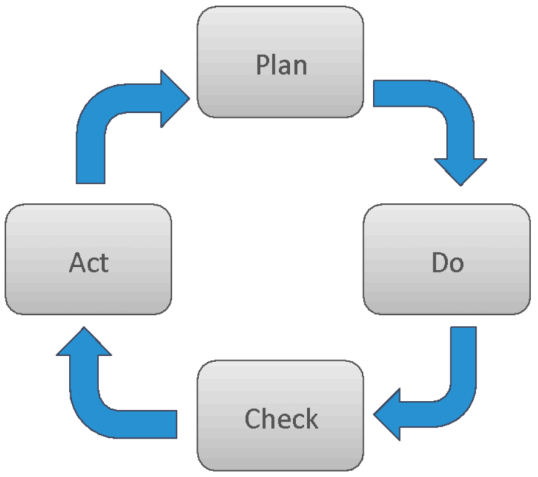
Het beveiligingsbeleid bevat de kaders voor beveiliging binnen theFactor.e. Hierin worden de doelstellingen, uitgangspunten, taken en verantwoordelijkheden evenals het procesmodel, dat binnen theFactor.e voor beveiliging wordt gehanteerd, beschreven. De richtlijnen zoals ISO 27001 bevatten de beveiligingseisen ten aanzien van informatiebeveiliging binnen theFactor.e. De richtlijnen vormen het basis beveiligingsniveau. De richtlijnen worden door de verantwoordelijken vertaald naar operationele maatregelen.

3.2 Procesmodel informatiebeveiliging

Een betrouwbare informatievoorziening vraagt om voortdurende aandacht. Wijzigingen in de organisatie en wijzigingen in de omgeving van de organisatie kunnen direct van invloed zijn op de betrouwbaarheidseisen die aan de informatievoorziening worden gesteld en de maatregelen die daarvoor moeten worden getroffen. De Deming cyclus wordt hiervoor gebruikt:

ISO/IEC 27001:2022 is gebaseerd op de Deming cycle:

- *Plan*: bepalen doelstellingen en maatregelen aan de hand van risicoanalyse
- *Do:* invoeren en uitvoeren beleid en maatregelen
- *Check*: bewaken en beoordelen doelstelling en maatregelen
- Act: bijsturen beleid en maatregelen (continue verbetering



1. Bepalen en vaststellen (plan)

In de deze fase wordt het beleid bepaald en de doelstellingen en uitgangspunten vastgesteld. Tevens wordt er bepaald welke methode voor risicobeoordeling er wordt toegepast en wordt deze beschreven. Daarnaast wordt de workshop risicobeoordeling voorbereid.

2. Invoeren en uitvoeren (do)

Het beleid wordt ingevoerd, geaccordeerd en uitgedragen. De risicobeoordeling en -behandeling wordt uitgevoerd en op basis van de uitkomsten wordt bepaald welke maatregelen er genomen moeten worden en er wordt een rapport opgesteld van de resultaten van de risicobeoordeling. Daarnaast wordt er een risico behandelplan opgesteld. Vervolgens worden de maatregelen geïmplementeerd.

3. Bewaken en beoordelen (check)

In deze fase wordt het beveiligingsproces bewaakt en wordt beoordeeld of de getroffen maatregelen in lijn zijn met de doelstellingen en uitgangspunten zoals geformuleerd in het beleid. De controle op de opzet, werking en bestaan van het beveiligingsproces leidt ertoe dat er verbeterpunten naar voren komen.

4. Evalueren en bijsturen (act)

In deze fase worden de verbeterpunten uit de vorige fase geëvalueerd. Aan de hand van de evaluatie wordt er bijgestuurd om het beveiligingsproces te verbeteren.

Alle documenten (dus ook dit document) moeten op systematische wijze goedgekeurd, beschermd, beheerd, gewijzigd en verspreid worden. Het documentbeheer moet naast deze doelen ertoe leiden dat de documentatie makkelijk leesbaar en identificeerbaar is, het aanwezig zijn van verouderde documenten wordt voorkomen en dat de documenten beschikbaar zijn voor diegenen die ze nodig hebben. Wijzigingen in documenten moeten worden gedaan door de eigenaar van het document. Tevens moet de eigenaar van een document de wijziging accorderen.

4. Organisatie voor informatiebeveiliging

4.1 Verantwoordelijkheden

Informatiebeveiliging is de verantwoordelijkheid van de directie. In dit hoofdstuk worden de taken, bevoegdheden en verantwoordelijkheden met betrekking tot het beveiligingsbeleid benoemd en wordt aangegeven bij welke functionarissen deze worden belegd. Door het expliciet beleggen van de verantwoordelijkheden wordt informatiebeveiliging verankerd in de bestaande organisatie.

4.2 Eindverantwoordelijk

De eindverantwoordelijkheid voor informatiebeveiliging ligt bij de directie van theFactor.e. De directie is verantwoordelijk voor het vaststellen van het beveiligingsbeleid en de daarin opgenomen richtlijnen, het coördineren van de implementatie van het beleid en de richtlijnen en het toezicht op de handhaving van deze beveiligingsrichtlijnen. Taken die hieruit voortvloeien, kunnen worden gedelegeerd aan specifieke functionarissen, die vervolgens een gedelegeerde verantwoordelijkheid dragen.

De directie is onder meer verantwoordelijk voor:

- Het hanteren van de beleidsuitgangspunten;
- Het aan de hand van de richtlijnen invoeren van informatiebeveiligingsmaatregelen;
- Het waarborgen van de naleving van het beveiligingsbeleid;
- Het bevorderen van het beveiligingsbewustzijn;
- Het controleren van het ISMS op basis van rapportages en uitvoeren van beoordelingen

Het is hierbij van belang dat de directie niet slechts incidenteel, maar structureel en planmatig aandacht besteedt aan informatiebeveiliging.

De directie voert voor de processen en systemen waar zij voor verantwoordelijk zijn eens per jaar of bij significante wijzigingen een risicoanalyse uit om eventuele wijzigingen in het beveiligingsbeleid aan te brengen. Risicoanalyses hebben zowel betrekking op de bestaande organisatie als op projecten en/of business cases. Nieuwe ontwikkelingen en inzichten aangaande informatiebeveiliging kunnen leiden tot wijzigingen in het beveiligingsbeleid.

De directie is integraal verantwoordelijk voor de interne controle op de uitvoering van het beleid, de richtlijnen en de maatregelen. Deze controles zijn zoveel mogelijk onderdeel van de reguliere processen.

4.3 Verantwoordelijkheid medewerkers

De medewerkers van theFactor.e hebben toegang tot informatie. Iedere medewerker is verantwoordelijk voor het in overeenstemming met het beleid en de richtlijnen omgaan met deze informatie en daarnaast voor alle aspecten van informatiebeveiliging binnen de eigen invloedssfeer.

4.4 Information Security officer

De Security Officer is verantwoordelijk voor de instandhouding van het informatiebeveiligingsbeleid. De Security Officer is de ‘spin in het web’ voor informatiebeveiliging binnen theFactor.e. Op hoofdlijnen omvat deze functie de volgende verantwoordelijkheden:

- Herijken en implementeren informatiebeveiligingsbeleid;
- Herijken tactische richtlijnen/standaarden informatiebeveiliging;
- Eens per jaar uitvoeren integrale risico analyse;
- Opstellen risico behandelplan, inclusief restrisico en acceptatiecriteria;
- Implementeren van maatregelen voortvloeiend uit het beleid en risico analyses;
- Coördineren van de implementatie van het gewenste niveau van informatiebeveiliging en het stimuleren van het beveiligingsbewustzijn;
- Adviseren van management over informatiebeveiliging en het rapporteren over de status van informatiebeveiliging binnen theFactor.e;
- Bewaken het niveau van informatiebeveiliging binnen theFactor.e.
- Coördinatie van interne audits. Hierbij rekening houdend met scheiding van taken; indien de Security Officer zelf betrokken is geweest bij het opstellen / de uitvoering van de maatregelen, is hij/zij niet geoorloofd de interne audit uit te voeren zonder dat er een andere auditor / security officer bij aanwezig is.

De Security Officer rapporteert aan de directie. De Security Officer ondersteunt de directie bij het plannen van de activiteiten voor informatiebeveiliging.

4.5 Rolmatrix

Naam	Rol	Taken	Wie
Directie	Bewust richting uitzetten op strategisch niveau, het IB 'apparaat' laten draaien, IB doelstelling communiceren, toezien op naleving van normen en beleid	Risico-adressering (accept, decrease, avoid, share) Middelen verstrekken, ISMS faciliteren en controleren (middels directiebeoordeling)	Directie
Chief Information Security Officer (CISO)	Hetzelfde als ISO, maar dan met eindverantwoordelijkheid	Zelfde als ISO	Bart Wesdorp
Information Security Officer (ISO)	Beleid opstellen, framework rond PDCA cycli opstellen & faciliteren	ISMS onderhouden Richting geven aan IS en IS-onderdelen Communicatie Training Evaluatie	Martijn Loonstra
Information Security Committee (ISCie)	Het "Wat" bepalen van de IS maatregelen en het definiëren van de interne norm en toezien hierop	Opstellen deel-maatregelen van ISMS Opstellen kwalificatie- en assessment criteria Controleren en evalueren betreffende IS-maatregelen Toezien op naleving en bepalen correctieve acties Het inventariseren en bijhouden van de belangrijkste informatiebronnen en -assets binnen de organisatie	CISO + ISO + Afgevaardigden vanuit: - software ontwikkeling - beheer - personeelszaken - ux/marketing
DevOps	(Informatie) systemen van de organisatie onderhouden en beheren	Logging, rechten beheren, overzicht over (informatie) systemen. Omvat super-user toegang tot alle systemen.	Hoofd DevOps + medewerkers aangesteld binnen DevOps team + mogelijke opsplitsing obv focus gebied
Project Security Officer	Het (helpen) implementeren van beheersmaatregelen en beleid binnen een project.	Risico-analyse Incidentherkenning Controle op effectiviteit Aanscherpen projectproces	Te bepalen per project
Medewerkers	Het volgen van het informatiebeveiligingsbeleid en het melden van afwijkingen en incidenten	Uitvoeren van het informatiebeveiligingsbeleid Uptodate blijven van geldende instructie en beleid	Alle TFE-ers en deta-vast

		Klanten en collega's scherp houden op eventuele kwetsbaarheden Melden van incidenten t.a.v. informatiebeveiliging	
Externen	Binnen projecten tijdelijke inhuurkracht met externe werkgever	Uptodate blijven van binnen project / organisatie geldende IB eisen	Alle tijdelijke krachten