Principes voor Informatiebeveiliging

Verwachtingen van de AFM ten aanzien van informatiebeveiliging

Lees verder

AFM

01
Inleiding

Lees meer

04
Bijlage

Lees meer

02
Doel van de principes

Lees meer

03
Principes voor informatiebeveiliging

Principe 1
Beleid

Principe 2
Governance

Principe 3
Identificeren van dreigingen en beoordelen van risico's

Principe 4
Mensen en cultuur

Principe 5
Technologie

Principe 6
Processen

Principe 7
Fysieke beveiliging

Principe 8
Data

Principe 9
Respons en herstel

Principe 10
Uitbesteding

Principe 11
Ketenperspectief

Lees meer

01
Inleiding

De Autoriteit Financiële Markten (AFM) publiceert principes voor onderwerpen waar zij toezicht op houdt. Principes bieden handvatten aan financiële ondernemingen en accountantsorganisaties (hierna ondernemingen) voor aspecten die volgens de AFM bijdragen aan de ontwikkeling van de sector. Op deze wijze vergroot de AFM de voorspelbaarheid van haar toezicht. Ondernemingen bepalen zelf hoe ze invulling geven aan de principes. Deze invulling kan verschillen afhankelijk van de omvang van de onderneming, het type dienstverlening en het soort product dat aangeboden wordt.

De AFM biedt nu principes aan op het gebied van informatiebeveiliging. De principes vervangen wettelijke vereisten niet. De principes bieden handvatten bij de invulling van wettelijke vereisten waarvoor de AFM dit van toegevoegde waarde acht. De reikwijdte van deze principes is opgenomen in de bijlage.

1.1 Het belang van informatiebeveiliging

De beheersing van informatiebeveiligingsrisico's wordt steeds belangrijker. Door de steeds verdere digitalisering van ondernemingen, maar ook door toenemende cyberdreiging.

Informatiebeveiliging is belangrijk voor de onderneming én voor haar klant. Klanten moeten namelijk kunnen vertrouwen op passende dienstverlening. Bovendien moeten ondernemingen integer en vertrouwelijk met hun gegevens omgaan. De AFM verwacht daarom dat ondernemingen zorgvuldig omgaan met informatiebeveiligingsrisico's.

De AFM helpt ondernemingen daarbij door met elf principes haar verwachtingen over informatiebeveiliging te duiden.

Bij haar toezicht op informatiebeveiliging streeft de AFM naar Europese en nationale convergentie in het toezicht op ondernemingen.

Klanten moeten kunnen vertrouwen op passende dienstverlening

02

Doel van de principes

De AFM heeft elf principes voor informatiebeveiliging[1] gedefinieerd. Elk principe is gericht op het realiseren van het hoofddoel:

Ondernemingen hebben passende maatregelen getroffen en procedures en processen geïmplementeerd om de continuïteit en betrouwbaarheid van de IT, de informatie en informatievoorziening te waarborgen en de gevolgen van eventuele beveiligingsincidenten tot een acceptabel en door de onderneming geaccepteerd niveau te beperken.

[1] De principes zijn opgesteld volgens internationaal geaccepteerde IT-risk-managementraamwerken, zoals ISO27001 en ISO27002, COBIT (COBIT 5, gepubliceerd door ISACA), National Institute of Standards and Technology Cybersecurity Framework (NIST) en richtlijnen van CPMI-IOSCO (Guidance on cyber resilience for financial market infrastructures) en het reeds bestaande toezicht op informatiebeveiliging door Nederlandse financiële ondernemingen.

Tussen de afzonderlijke principes bestaat samenhang en een wisselwerking om dat doel te bereiken. Elk principe beslaat een onderdeel van informatiebeveiliging. Die onderdelen zijn:

1. **Beleid**
2. **Governance**
3. **Identificeren van dreigingen en beoordelen van risico's**
4. **Mensen en cultuur**
5. **Technologie**
6. **Processen**
7. **Fysieke beveiliging**
8. **Data**
9. **Respons en herstel**
10. **Uitbesteding**
11. **Ketenperspectief**

De basis van informatiebeveiliging wordt gevormd door beleid, governance en het identificeren van dreigingen en beoordelen van risico's. Het dreigingsbeeld is niet statisch. Daarom is het belangrijk om ervoor te zorgen dat een onderneming haar informatiebeveiliging voortdurend actualiseert en verbetert.

Met een goed informatiebeveiligingsbeleid, zorgvuldige governance en het voortdurend identificeren en analyseren van dreigingen en risico's kunnen de juiste maatregelen worden getroffen op het gebied van: mensen en cultuur, technologie, processen en fysieke beveiliging. Het doel hiervan is voldoende beveiliging van de hierbij verwerkte en geproduceerde data en informatie.

Informatiebeveiligingsincidenten kunnen desondanks nog plaatsvinden. Daarom moeten ondernemingen respons- en herstelmaatregelen kunnen uitvoeren om de impact hiervan te beperken.

De informatiesystemen van ondernemingen zijn verweven met andere, externe partijen. Daarom zijn niet alleen risico's en maatregelen van de eigen onderneming relevant voor de onderneming, maar ook die van betrokken externe partijen.

> Het is belangrijk om ervoor te zorgen dat een onderneming haar informatiebeveiliging voortdurend actualiseert en verbetert

03

Principes voor informatiebeveiliging

1.
Beleid

Een actueel informatiebeveiligingsbeleid beschrijft een samenhangend geheel van maatregelen, procedures en processen waarmee informatiebeveiligingsrisico's worden beheerst.

In het beleid stelt de onderneming haar doelstellingen voor informatiebeveiliging vast en de wijze waarop zij deze doelstellingen behaalt. De AFM moedigt ondernemingen aan gebruik te maken van internationaal geaccepteerde raamwerken voor informatiebeveiliging en cybersecurity[2] bij het opstellen van het informatiebeveiligingsbeleid. De AFM ziet cybersecurity als integraal onderdeel van informatiebeveiliging.

Het beleid beschrijft de uitgangspunten, de IT-standaarden die door de onderneming worden gehanteerd en de verantwoordelijkheden, procedures en processen om informatiebeveiliging in te bedden in de onderneming. Het informatiebeveiligingsbeleid is in elk geval van toepassing op de IT-assets[3] en processen in eigen beheer, persoonlijke gegevensdragers van medewerkers (voor zover deze geautoriseerd zijn voor zakelijk gebruik), digitale producten van de organisatie en de uitbestede IT-assets en processen.

In het beleid staat hoe de onderneming de eisen bepaalt op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid[4] van IT-assets en processen, inclusief fysieke locaties en data. De specifieke maatregelen die volgen uit het informatiebeveiligingsbeleid zijn in lijn met deze eisen.

Het informatiebeveiligingsbeleid blijft actueel door dreigingen en risico's periodiek te evalueren. Extra evaluatie vindt plaats als er nieuwe risico's ontstaan of de grootte van risico's of dreigingen significant toeneemt.

2.
Governance

De onderneming richt een governance structuur in die effectieve informatiebeveiliging mogelijk maakt.

Het bestuur van een onderneming is verantwoordelijk voor informatiebeveiliging en heeft de expertise om deze verantwoordelijkheid te nemen. De belangrijkste informatiebeveiligingsrisico's, dreigingen en incidenten zijn bij het bestuur van de onderneming bekend.

Als onderdelen van de onderneming niet voldoen aan het informatiebeveiligingsbeleid, worden aanvullende maatregelen getroffen óf kan op basis van een zorgvuldige afweging besloten worden de risico's van niet-naleving te aanvaarden.

De invulling van de organisatiestructuur voor informatiebeveiliging is afgestemd op het bedrijfsmodel, de omvang en complexiteit van de onderneming, de kenmerken van de informatie en data die de onderneming creëert of verwerkt en de bijbehorende informatiebeveiligingsrisico's.

Een heldere taakverdeling en beschikbaarheid van voldoende deskundigheid en ervaring zijn cruciaal voor de kwaliteit van risicobeoordelingen en de effectiviteit van de informatiebeveiligingsmaatregelen. De rollen en verantwoordelijkheden op het gebied van het inrichten, beheren en controleren van informatiebeveiliging zijn daarom helder belegd[5]. De onderneming heeft voldoende capaciteit, kennis en ervaring tot haar beschikking op het gebied van informatiebeveiliging om invulling aan deze rollen en verantwoordelijkheden te geven.

[2] Zoals bijvoorbeeld ISO27001 en ISO27002, COBIT, CPMI-IOSCO en NIST.
[3] Alle aangekochte of zelf ontwikkelde IT hardware en software.
[4] BIV is het acroniem voor Beschikbaarheid, Integriteit, Vertrouwelijkheid. Een BIV-classificatie is een indeling die binnen de informatiebeveiliging wordt gehanteerd, waarmee de eisen aan de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen wordt geclassificeerd.
[5] Zoals bijvoorbeeld in een RACI-matrix.

3.
Identificeren van dreigingen en beoordelen van risico's

Informatiebeveiliging is ingericht op basis van een actueel inzicht in bestaande dreigingen en risico's, de potentiële impact van bestaande dreigingen op de onderneming en de risicobereidheid van de onderneming.

Op basis van inzicht in bestaande dreigingen en risico's implementeert de onderneming maatregelen op de gebieden die onderdeel zijn van principe 4 tot en met 8. Zo geeft zij invulling aan haar informatiebeveiligingsbeleid.

Informatiebeveiliging is dynamisch. Technologie en bedreigingsfactoren ontwikkelen zich continu. Daarmee ontstaan nieuwe risico's. De onderneming actualiseert daarom haar risicobeoordeling periodiek op basis van inzicht in de voor de onderneming relevante dreigingen op het gebied van informatiebeveiliging. Een manier om inzicht in bestaande risico's te krijgen is door de effectiviteit van de risicobeheersingsmaatregelen te toetsen, uitgaande van bestaande dreigingen. Zowel interne als externe bronnen kunnen van toegevoegde waarde zijn in het bepalen van deze dreigingen.

De frequentie en diepgang van de risicobeoordeling is afgestemd op het bedrijfsmodel, de omvang en complexiteit van de onderneming en de kenmerken van de informatie en data die door de onderneming wordt gecreëerd of verwerkt. De onderneming weegt in haar risicobeoordeling de belangen mee van de eigen onderneming en de belangen van haar stakeholders, zoals haar klanten en van de sector waarin zij werkzaam is.

Op basis van inzicht in bestaande en voorzienbare dreigingen en risico's beoordeelt de onderneming de mate waarin haar informatiebeveiligingsmaatregelen toereikend zijn en treft de benodigde additionele maatregelen en accepteert (tijdelijk) risico's. Geaccepteerde risico's evalueert de onderneming periodiek opnieuw. De onderneming hanteert hiertoe wettelijke vereisten en haar doelstellingen op het gebied van beschikbaarheid, integriteit en vertrouwelijkheid van processen, systemen, data en informatie.

4.
Mensen en cultuur

De onderneming onderkent het risico van menselijk handelen voor informatiebeveiliging en creëert en ondersteunt een cultuur waarin medewerkers zich bewust zijn van het risico op informatiebeveiligingsincidenten en hierover open communiceren.

Mensen zijn een belangrijke schakel in informatiebeveiliging. Onverantwoord gedrag of onbewust gedrag van mensen kan leiden tot informatiebeveiligingsincidenten. Dit erkent de onderneming en neemt doeltreffende maatregelen. De onderneming richt processen in zodat mensen effectief bijdragen aan adequate informatiebeveiliging en om meldingen over incidenten door medewerkers naar behoren te behandelen. In aanvulling hierop maakt een onderneming bijvoorbeeld gebruik van bewustwordingsprogramma's en trainingen. De effectiviteit van deze maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die een onderneming treft.

De onderneming erkent het risico van menselijk handelen op de effectiviteit van het informatiebeveiligingsbeleid en treft adequate maatregelen om dit risico te beperken. Hierin worden zowel de risico's als gevolg van interne factoren (bijvoorbeeld interne fraude) als risico's als gevolg van externe factoren (bijvoorbeeld phishing via e-mail) meegenomen. Om deze risico's te beperken, kunnen ondernemingen technische, procedurele en fysieke maatregelen treffen. Deze maatregelen ondersteunen medewerkers om hun verantwoordelijkheden op het gebied van informatiebeveiliging te vervullen. Eventuele restrisico's worden afgewogen tegen de kosten en impact van aanvullende maatregelen om deze risico's te beperken.

Het bestuur en (senior) management van de onderneming draagt het belang van informatiebeveiliging uit en maakt medewerkers bewust van de bestaande dreigingen. Alle medewerkers worden op verschillende manieren actief bewust gemaakt en opgeleid om hun verantwoordelijkheid op het gebied van informatiebeveiliging te nemen.

5.
Technologie

Bij de implementatie en het onderhoud van systemen wordt het uitgangspunt ‘secure by design’ toegepast.

De onderneming wordt aangemoedigd om internationale technologiestandaarden te gebruiken om informatiebeveiliging in te bedden in het ontwerp van de IT-architectuur en systemen. Informatiebeveiligingsrisico’s worden als realistische scenario’s beschouwd, waar vanaf de ontwerpfase rekening mee gehouden wordt. De IT-architectuur en systemen zijn ontworpen en ingericht om veilig te zijn.

De onderneming onderkent de risico’s van het gebruik van nieuwe en verouderde technologie en heeft maatregelen getroffen om deze risico’s te beperken. Wijzigingen in de onderneming en de IT- infrastructuur voert zij op zo’n manier door dat informatierisico’s tot een acceptabel niveau worden gereduceerd conform beleid en de risicobereidheid van de onderneming.

Bij de implementatie en tijdens het onderhoud van systemen weegt de onderneming de wendbaarheid van de IT-infrastructuur mee om te voorkomen dat er afhankelijkheden ontstaan van niet meer vervangbare systemen.

De effectiviteit van technische maatregelen test een onderneming periodiek, ook in combinatie met de overige informatiebeveiligingsmaatregelen die zijn getroffen.

6.
Processen

De inrichting van bedrijfsprocessen waarborgt de beschikbaarheid, integriteit en vertrouwelijkheid van processen en de hierin gebruikte systemen.

Alle processen van de onderneming zijn zo ingericht dat deze waarborgen bevatten om de beschikbaarheid, integriteit en vertrouwelijkheid van deze processen en systemen (en de verwerkte data) te garanderen in lijn met het beleid en de risicobereidheid van de organisatie. Informatiebeveiliging is een integraal onderdeel van de administratieve organisatie en interne beheersing van de onderneming. De effectiviteit van de maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen. Bevindingen worden opgevolgd en gecommuniceerd naar het (senior) management van de onderneming.

Voor de inrichting van IT-ontwikkel- en beheerprocessen worden ondernemingen aangemoedigd gebruik te maken van internationaal geaccepteerde raamwerken voor informatiebeveiliging. De onderneming implementeert processen om informatiebeveiligingsrisico’s te identificeren en in lijn te brengen met het informatiebeveiligingsbeleid. Daarnaast implementeert de onderneming processen om dreigingen te monitoren en incidenten te detecteren en hierop adequaat te reageren (zie principe 9).

7.
Fysieke beveiliging

Het ontwerp en de inrichting van de faciliteiten en apparatuur van de onderneming is in lijn met de eisen aan informatiebeveiliging.

De onderneming heeft fysieke maatregelen getroffen in aanvulling op technische en procedurele maatregelen, bijvoorbeeld om de toegang tot faciliteiten en apparatuur te beperken. Fysieke maatregelen ter bescherming van faciliteiten en apparatuur zijn getroffen op basis van een analyse van de risico's van externe factoren (zoals de kans op natuurrampen), menselijke factoren (zoals ongeautoriseerde toegang) en crisissituaties (als gevolg van bijvoorbeeld de uitval van elektriciteit).

De informatiebeveiligingsrisico's van faciliteiten en apparatuur zijn opgesteld conform het informatiebeveiligingsbeleid. De onderneming test de effectiviteit van deze maatregelen periodiek getest in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen

8.
Data

Tijdens de volledige levenscyclus van data en informatie zijn maatregelen getroffen om te voldoen aan de relevante beveiligingseisen.

Informatiebeveiligingsdoelstellingen zijn gedefinieerd om de benodigde beschikbaarheid, integriteit en vertrouwelijkheid van data en informatie te waarborgen. Deze zijn vertaald in maatregelen om hieraan te kunnen voldoen gedurende de volledige levenscyclus van data. Deze maatregelen hebben betrekking op zowel de opslag, het gebruik als het transport van data via communicatiekanalen. De effectiviteit van deze maatregelen wordt periodiek getest, ook in combinatie met de overige informatiebeveiligingsmaatregelen die door de onderneming zijn getroffen.

De verantwoordelijkheid voor databronnen en het bewerken van die bronnen is belegd binnen de organisatie. Dit betreft de adequate informatiebeveiliging van actuele en historische data. Wettelijke eisen en intern beleid rondom de beschikbaarheid, integriteit en vertrouwelijkheid van data worden door de onderneming in acht genomen. Dit geldt ook voor systeemtransformaties en datamigraties zodat historische data en de samenhang tussen data elementen beschikbaar blijven conform de eisen die voortvloeien uit wetgeving en de doelstellingen voortkomend uit het informatiebeveiligingsbeleid.

9.
Respons en herstel

De onderneming is voorbereid op informatiebeveiligingsincidenten om de impact hiervan op de bedrijfsvoering van de onderneming te beperken. Wanneer zich een informatiebeveiligingsincident voordoet, neemt de onderneming tijdig en doeltreffende respons- en herstelmaatregelen.

De onderneming beschikt over processen en plannen die worden geactiveerd op het moment dat een informatiebeveiligingsincident wordt gedetecteerd. Deze processen en plannen bevatten in elk geval maatregelen om (1) het incident te stoppen, (2) de negatieve impact te beperken, (3) de schade te herstellen en (4) hier goed over te communiceren.

Er vindt evaluatie plaats tijdens en na de herstelactiviteiten. De opgedane inzichten worden verwerkt in het informatiebeveiligingsbeleid, bestaande processen en systemen en de communicatie naar en opleiding van medewerkers.

10.
Uitbesteding

De onderneming is verantwoordelijk voor de informatiebeveiliging van uitbestede processen en systemen.

Een onderneming die processen of IT-systemen uitbesteedt aan een interne partij (binnen de groep waar de onderneming deel van uitmaakt) of aan een externe partij, is zelf verantwoordelijk voor de informatiebeveiliging van deze processen en systemen. Voordat IT-infrastructuur en/of processen uitbesteed worden, voert de onderneming een gedegen onderzoek naar de informatiebeveiliging van de toeleverancier uit, waarbij de omvang en diepgang van het onderzoek is afgestemd op risico's voor de informatiebeveiliging van de onderneming.

De onderneming is zich bewust van de gevolgen van uitbesteding voor de rollen en verantwoordelijkheden, risicomanagement en ketenintegratie. De analyse van deze risicofactoren wordt door de onderneming regelmatig geactualiseerd. De onderneming bepaalt de impact van uitbesteding op de beschikbaarheid, integriteit en vertrouwelijkheid van processen, systemen, data en informatie en neemt passende beheersmaatregelen.

De onderneming maakt heldere contractuele afspraken over de samenwerking en de verdeling van de verantwoordelijkheden op het gebied van informatiebeveiliging. Dit betreft tevens de bevoegdheid om audits uit te voeren bij de leverancier.

11.
Ketenperspectief

De onderneming past een integrale ketenbenadering toe bij het bepalen van informatiebeveiligingsrisico's en de benodigde beheersmaatregelen.

De integrale ketenbenadering is het beheersen van meer dan alleen de risico's die ontstaan in de eigen IT-omgeving. De keten bestaat uit verschillende schakels van interne en externe partijen, waaronder de klant en toezichthouders. De onderneming past een integrale ketenbenadering toe wanneer zij aandacht heeft voor haar eigen plaats in de keten en de afhankelijkheden van andere ketenpartijen.

De onderneming hanteert als uitgangspunt dat ondernemingen in dezelfde sector en binnen een keten coalitiegenoten zijn in het beschermen van de sector tegen externe informatiebeveiligingsrisico's. Zwakheden van een ketenpartij hebben mogelijk gevolgen voor andere partijen in dezelfde keten. Om deze risico's in kaart te brengen, participeert de onderneming indien mogelijk en relevant in informatiebeveiligingstesten die door autoriteiten voor sectoren of ketens worden georganiseerd.

De AFM moedigt ondernemingen aan om binnen ketens en binnen de sector kennis en informatie uit te wisselen over informatiebeveiligingsrisico's en dreigingen.

Op basis van inzicht in ketenafhankelijkheden, streeft de onderneming ernaar afspraken te maken over informatiebeveiliging met andere partijen in de keten. Dit betreft onder meer afspraken om de impact van grootschalige incidenten te beperken voor de getroffen onderneming en de keten als geheel. Indien deze afspraken niet bestaan, treft de onderneming geschikte maatregelen om dit risico te beperken.

04
Bijlage

Reikwijdte principes voor informatiebeveiliging

De reikwijdte van de principes voor informatie-beveiliging betreft op het moment van publicatie:

- Alternatieve beleggingsinstellingen (ABI)
- Beheerders van een ABI
- Instellingen voor collectieve beleggingen in effecten (ICBE)
- Beheerders van een ICBE
- Beleggingsondernemingen
- Bewaarders
- Financiële dienstverleners (voor zover het geen bank, verzekeraar of financiële instelling betreft)
- Pensioenbewaarders
- Verleners van datarapporteringsdiensten
- Gereglementeerde markten
- Accountantsorganisaties

Heeft u vragen of opmerkingen over deze beleidsuiting?

Stuur een e-mail naar redactie@afm.nl

Autoriteit Financiële markten
Vijzelgracht 50, 1017 HS Amsterdam

Telefoon
020 797 2000

www.afm.nl

Volg ons:

De tekst van deze publicatie is met zorg samengesteld en is informatief van aard. U kunt er geen rechten aan ontlenen. Door veranderende wet- en regelgeving op nationaal en internationaal niveau is het mogelijk dat de tekst niet actueel is op het moment dat u deze leest. De Autoriteit Financiële Markten (AFM) is niet aansprakelijk voor de eventuele gevolgen – bijvoorbeeld geleden verlies of gederfde winst – ontstaan door of in verband met acties ondernomen naar aanleiding van deze tekst.

© Copyright AFM 2019
alle rechten voorbehouden