FISP - Federal Information Security Policy

Handleiding voor de controle en de beveiliging van de fysieke toegangen

21/11/2019

FISPDOC02 V1.0

FISP Werkgroep

.be

INHOUDSTAFEL

Inhoud van dit document

Oriëntatie van het document

Deze richtlijn geeft een overzicht van de belangrijkste principes m.b.t. de fysieke beveiliging en de beveiliging van de omgeving van de organisatie.

Veiligheidsdoel van het document

De doelstelling van deze richtlijn is om minimale maatregelen te geven ter beveiliging van informatie tegen onbevoegde fysieke toegang, schade aan en manipulatie van informatie en informatie verwerkende faciliteiten van de organisatie.

Toepassingsgebied

Dit beleid voor informatiebeveiliging is toepasselijk voor alle informatie die er circuleert in de federale organisaties.

Vertrouwelijkheid van het document

Publieke verspreiding

Vrijwaring

Dit is een richtlijn op basis van de internationale praktijken m.b.t. minimale maatregelen voor fysieke beveiliging in een context van informatiebeveiliging. Indien u deze richtlijn voor uw organisatie wilt toepassen, moet u eerst een beoordeling maken en controleren of andere wettelijke beperkingen, regels of praktijken van toepassing zijn op uw organisatie. Pas het beveiligingsbeleid aan, in lijn met uw organisatie!

Verantwoordelijkheden

Elke organisatie onderschrijft de beschreven maatregelen, voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie.

Eigenaar

De eigenaar van dit document is de FISP-werkgroep.

Inleiding

Fysieke beveiliging en beveiliging van de omgeving, impliceren maatregelen die betrekking hebben op het verhinderen of limiteren van fysieke gebeurtenissen zoals ongeautoriseerde toegang, verlies, vandalisme en inbraak. Daarnaast heeft het ook betrekking op beveiliging tegen omgevingsfactoren zoals natuurrampen, bliksem- en wateroverlast, ontvallen van nutsvoorzieningen, … De waarde van apparatuur, de gevoeligheid van gegevens en discontinuïteit van gegevensverwerking, vormen redenen genoeg voor het nemen van de gewenste maatregelen op het gebied van fysieke beveiliging.

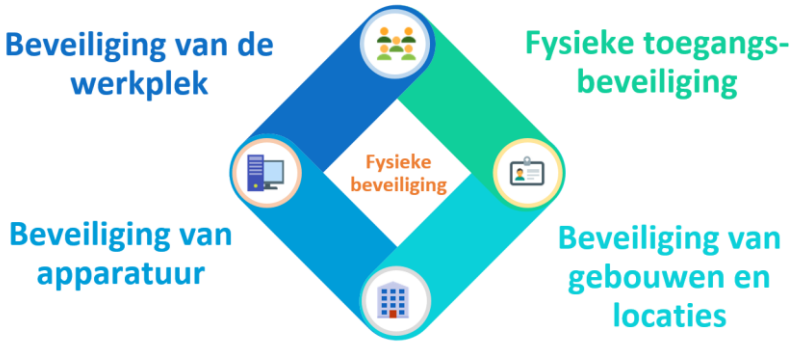
Fysieke beveiliging vereist aldus extra aandacht tijdens de inrichting van locaties, gebouwen, ruimtes, etc. Deze bijzondere aandacht is in de eerste plaats van belang voor kritieke ruimtes, zoals locaties met technische apparatuur, datacenters,… Daarnaast moet er ook extra aandacht besteed worden aan fysieke toegangscontrole, veiligheidsmaatregelen op de werkplek en de beveiliging van apparatuur.

Het doel van dit beleid is om minimale maatregelen te geven ter beveiliging van informatie tegen onbevoegde fysieke toegang tot, schade aan en manipulatie van informatie en informatie verwerkende faciliteiten van de organisatie. Het beleid fysieke beveiliging en beveiliging van de omgeving is ontwikkeld, rekening houdend met bestaande normen zoals ISO 27001 en ISO 27002.

De bedrijven in gebouwbeheer moet maatregelen treffen om een minimum beveiliging te waarborgen. Deze maatregelen moeten vervolgens meegedeeld worden aan organisaties die de gebouwen gebruiken. Organisaties die gebouwen gebruiken, moeten de maatregelen voor het beheer van gebouwen integreren in hun risicoanalyse om het risiconiveau te bepalen. De maatregelen moeten tot slot geïntegreerd worden in het beleid van de organisatie die het gebouw gebruikt.

De minimale maatregelen die in dit beleid vooropgesteld worden zijn gekoppeld aan een risicobeoordeling of impact analyse, die door de organisaties moeten ondernomen worden. Vanuit deze risicobeoordeling kan de organisatie vervolgens een gewenst beveiligingsniveau definiëren

Elke organisatie onderschrijft de beschreven maatregelen, voor alle informatie en informatiesystemen onder de verantwoordelijkheid van de organisatie. Het is bovendien belangrijk om te verduidelijken dat de voorgestelde minimale maatregen betrekking hebben op informatiebeveiliging en geen betrekking hebben op het takenpakket van de preventieadviseur. Het is echter noodzakelijk dat er een goede samenwerking is tussen de verantwoordelijke voor informatiebeveiliging en de preventieadviseur. De procedures en processen om de maatregelen tot stand te brengen moeten door de organisatie gedefinieerd en gepland worden (bv. met behulp van ITIL).



Beveiliging van ruimten

Algemeen

Elke organisatie moet de nodige maatregelen treffen ter voorkoming van verlies, schade, diefstal of manipulatie van de informatie in een organisatie. De organisatie moet fysieke maatregelen nemen in lijn met de specificaties en functie van de gebouwen en locaties.

Gebouwen en locaties moeten voldoen aan volgende infrastructurele vereisten en bouwkundige voorzieningen:

1) weerstand aan calamiteiten (brand, blikseminslag, storm, hagel, overstroming/waterlekken, aardschok,..);

2) wand-, vloer- en plafondconstructies moeten voldoen aan de eisen betreffende brandwerendheid en voldoende afgewerkt zijn (stof, brand, rook);

3) voorzieningen moeten worden geconfigureerd om te voorkomen dat vertrouwelijke informatie of activiteiten zichtbaar zijn en hoorbaar van buiten;

4) externe elektriciteitstoevoer met voeding vanaf twee zijden;

5) implementatie van maatregelen tegen schade door onder- of overspanning;

De beheerder van het gebouw moet alle informatie, betreffende de infrastructuur, bouwkundige voorzieningen en de oplossingen voor technische storingen, op een eenvoudige manier ter beschikking stellen.

Interne elektriciteitsvoorziening

Interne elektriciteitsvoorziening is noodzakelijk voor kritische ruimte waar de meest kritische bedrijfsprocessen verder gezet moeten worden. Het is bovendien noodzakelijk om gebruik te maken van UPS (+ generator indien nodig)zodat de netspanning niet uitvalt.

Deze installatie voor interne elektriciteitsvoorziening moet jaarlijks minsten één keer getest worden op goede functionaliteit. Het onderhoud van deze installatie dient volgens de voorschriften te gebeuren.

Telecommunicatie-infrastructuur

De interne (tele)communicatiebekabeling en -verdeelpunten moeten:

1) onbereikbaar zijn voor onbevoegden;

2) afgeschermd zijn van voedingskabels, bliksemafleiders, Tl-buizen, spoelen, etc.

Voor bedrijfsprocessen, die kritische datacommunicatieverbindingen nodig hebben, moeten back-upvoorzieningen worden getroffen.

Klimaatbeheersing

Klimaatbeheersing van de verschillende ruimtes is essentieel. De luchtbehandeling van kritische ruimtes met gevoelige apparatuur moet afgesloten zijn van de overige ruimtes. Het gevaar van aanzuiging van gevaarlijke stoffen moet bovendien ook beperkt blijven. Er moet ook rekening gehouden met temperatuur schommeling in kritische ruimtes. Tot slot moet een schakelaar voorzien worden zodat men bij alarmering de luchtventilatie handmatig 'UIT' kan schakelen.

Brandbeveiliging

Voor brandbeveiliging gelden een aantal vereisten rond preventie, detectie en bestrijding. Deze fysieke beveiligingsmaatregelen worden periodiek geïnspecteerd.

Preventieve voorzieningen

Brand- en rookontwikkeling moet te allen tijde beperkt worden. Tijdens de bouw en inrichting van kritische ruimtes moeten de toegepaste materialen dus zorgvuldig gekozen worden. Brandwerende scheidingen zijn bovendien ook van essentieel belang. De aansluitingen van wanden en plafonds, doorvoer van luchtkanalen, elektriciteit- en andere leidingen, verdienen ook extra aandacht (bijvoorbeeld door rookdicht sluitende brandkleppen).

Ter voorkoming van blikseminslag moeten er ook bliksemafleiderinstallaties geïnstalleerd worden om schade door blikseminslag zoveel mogelijk te voorkomen.

Tot slot is een wettelijk ingericht rookverbod in alle organisaties - er is een rookverbod in alle kritische (data) ruimtes.

Branddetectie en –signalering

Er moet automatische (en handmatige) detectieapparatuur aanwezig zijn in de kritische ruimtes (tevens onder verhoogde vloeren, boven verlaagde plafonds etc.) en in ruimtes met hoge brandveiligheidseisen. Een regelmatige controle dient plaats te vinden op de werking van deze detectieapparatuur. Overigens moet deze detectieapparatuur voorzien zijn van een eigen noodstroomvoorziening.

Brandbestrijding

Instructies betreffende brandbestrijding moeten aanwezig zijn zodat iedereen weet hoe te handelen in geval van brand. Deze instructies hebben aandacht voor:

- de wijze van alarmering, en ontruiming;
- redden van in gebruik zijnde informatiedragers en het uitschakelen van computerapparatuur;
- gebruik van (automatische) brandblussers, en gebruik van luchtbehandelingsinstallatie.

De kritische ruimtes moeten voorzien zijn van (een) automatische blusinstallatie(s). Het moet overigens wel mogelijk zijn om deze handmatig uit te zetten. Bij de keuze voor de blusinstallatie moet men rekening houden met de apparatuur en de eventuele aanwezigheid van medewerkers en/of bezoekers.

Waterschade

Om waterschade in kritische ruimtes te voorkomen mogen er geen waterleidingen aanwezig zijn in deze kritische ruimtes. Men moet bovendien automatische vochtdetectors instaleren in de directe omgeving van kritische apparatuur. Er dient echter wel een uitzondering gemaakt te worden voor brandblusinstallaties en de koeling apparatuur aanwezig in de data centers.

Fysieke toegangscontrole

Onbevoegde toegang tot, schade aan en inmenging in informatie en informatie verwerkende faciliteiten van de organisatie moeten te allen tijde voorkomen worden.

Aangezien de openbare organisatie een open instelling is met een mogelijke grote omloop van personen en sommige gebouwen een publieke functie hebben is een consequente beperking van toegankelijkheid niet overal voor de hand liggend.

Volgende maatregelen worden voorgesteld om de grote gebruikersstroom op een veilige en gebruiksvriendelijke manier te organiseren:

1) Door middel van sleutels (mechanisch of digitaal) en dit volgens een strikt sleutelplan;

2) Door middel van persoonlijke toegangsbadges (inclusief tijdelijke toegangsbadges voor bezoekers).

Voor toegangscontrole gelden de volgende eisen:

1) Verplichting voor werknemers tot identificatie. De toegangsbadges zijn persoonsgebonden. Blanco toegangsbadges of niet toegewezen badges moeten veilig opgeborgen worden.

2) Toegang tot zones waar vertrouwelijke informatie wordt verwerkt, moet worden beperkt tot geautoriseerde personen. Men kan de toegang tot deze zones beperken door een authenticatiemechanisme bestaande uit een PIN om toegang te krijgen tot de organisatie en een badge om het gebouw te verlaten. Andere mogelijkheden zijn biometrische herkenning,het 4-eyes principe,...

3) Bezoekers moeten vooraf door de ontvangende medewerker worden aangemeld, waarbij moet worden aangegeven of de betreffende bezoeker bij binnenkomst mag doorlopen of moet worden afgehaald door de ontvangende medewerker.

4) Bezoekers moeten geregistreerd worden (datum en tijdstip van binnenkomst en vertrek), vb. digitaal of door het invullen van een bezoekerslog.

5) Niet geaccrediteerd schoonmaak- en onderhoudspersoneel mag alleen in kritische zones werken onder permanent toezicht van medewerkers.

6) Bewaking van toegangscontrole door middel van camerabewaking en/of bewakingspersoneel.

Beveiligde zone

Na het analyseren van risico's kan het praktischer zijn om verschillende beveiligingszones te creëren in een organisatie. De zones en ruimtes zijn vervolgens beschermd afhankelijk van hun impact in de organisatie.

Men doet er goed aan om onderlinge praktijkafspraken te maken tussen de verschillende zones. Een "masterplan" toegangsbeveiliging of vergelijkbaar document (met een plan van aanpak, procesbeschrijvingen/ procedures, ...) is hier zeker op zijn plaats.

Er kunnen drie globale zones geïdentificeerd worden:

Type	Beschrijving
Publieke zone	In de publieke zones kan men onvoldoende fysieke controles uitvoeren. Men kan in deze zone het vooropgestelde veiligheidsniveau niet garanderen. Men kan de mobiele werkplek als een publieke zone beschouwen.
professionele zone	De niet-publieke ruimten, gebouwen en werkplek vallen onder de professionele zone. De ruimtes die onder deze zone vallen hebben extra beveiligingsmaatregelen nodig t.o.v. de publieke zone. De extra beveiligingsmaatregelen worden genomen in lijn met de BIV – classificatie (beschikbaarheid, integriteit en vertrouwelijkheid).
Kritieke zones	Het gaat hier om gecontroleerde zone met extra beveiligingsmaatregelen t.o.v. de professionele zone. De beveiligingsmaatregelen zijn o.a. afhankelijk van de impact van verlies, diefstal, manipulatie.. van informatie op de organisatie.

De vereisten voor zone beveiliging (professionele zone en kritieke zone)

1) De zones moeten functioneel van elkaar gescheiden zijn.

2) Het is verboden om ongeautoriseerde toegang te verlenen. Er moeten toegangsbeveiligingen worden aangebracht om ruimte te beschermen waar zich gevoelige of kritische informatie en ICT voorzieningen bevinden.

3) Voorkomen of tijdig detecteren van ongeautoriseerd gebruik van de toegang naar kritische zones.

4) Personeel, bezoekers en leveranciers hebben uitsluitend toegang tot de zones waar hun aanwezigheid noodzakelijk is omwille van hun werkzaamheden.

5) Het is noodzakelijk om gescheiden ingangen voor personen en goederen (aparte laad- en loszones) te voorzien. Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, moeten worden beheerst en indien mogelijk worden afgeschermd van kritieke zones om onbevoegde toegang te voorkomen.

6) De toegangsmaatregelen voor de fysieke beveiliging van de zones moeten voorzien zijn van de nodige controle- en monitoring mechanismen:
   - detectie openstaande deuren;
   - klem beveiliging automatische deuren;
   - camerabewaking;

- signalisatie (brand, wateroverlast);
- inbraak beveiliging,..

7) De apparatuur voor toegangscontrole moet voorzien zijn van een noodstroomvoorziening, zodat de veiligheid van personen gegarandeerd blijft, ingeval van een stroomonderbreking.

8) De implementatie van incidentprocessen is noodzakelijk om de aanwezige personen bij te staan. (personeel, gebouw verantwoordelijken en bezoekers, baliepersoneel en bewakingsagenten,...)

Beveiliging van de (mobiele) werkplek

In samenloop met maatregelen ter beveiliging van locaties, moeten de nodige maatregelen ook genomen worden voor de werkplek. De werkplek, of het werkstation wordt daarom beschouwd als een virtuele locatie.

1) Kantoor:

   Op kantoor maakt de werkplek onrechtstreeks gebruik van maatregelen die niet initieel voor de werkplek genomen zijn, maar deze wel een extra bescherming bieden. Het gaat hier om toegangsbewaking, centrale back-up (beveiliging tegen verlies van informatie), brandbeveiliging, beveiliging tegen stroomonderbreking, functiescheiding, enzovoorts.

2) Mobiele werkplek:

   Op de mobiele werkplek worden in het algemeen minder of geen beveiligingsmaatregelen getroffen. De thuissituatie kan men aanzien als een publieke ruimte (vanuit het standpunt van de organisatie). Men moet een kopie van het beleid, voor de beveiliging van apparatuur buiten de organisatie, bezorgen aan de werknemer. Het is bovendien noodzakelijk om briefings en sensibiliseringscampagnes te ondernemen om de werknemers te informeren.

Architectuur van de werkplek

De architectuur en de beveiligingsmaatregelen van de werkplek moeten rekening houden met:

- het dynamisch aspect van de fysieke locatie (kantoor, op en tijdens verplaatsing);
- het mobiele aspect van de werkplek (Portables).

De te nemen maatregelen zijn toepasselijk voor de fysiek moeilijkst te beveiligen locaties:

1) **statische toestellen;**
   Dit zijn toestellen die de beveiligde fysieke locatie (inclusief het beveiligde netwerk) van de organisatie niet verlaten.
2) **mobiele toestellen**.
   Dit zijn toestellen die de beveiligde fysieke locatie van de organisatie, of het beveiligde netwerk verlaten.

Toestellen die op regelmatige basis mee op verplaatsing worden genomen of regelmatig verbonden worden met een ander netwerk dan het beveiligde netwerk van de organisatie, zijn het gevoeligst.

Beveiligingsmaatregelen verschillen naargelang het type werkstation dat op de werkplek gebruikt wordt:

1) Een **kiosk toestel** (is niet verbonden met het overheidsnetwerk). Bijvoorbeeld een computer verbonden met het internet die ter beschikking wordt gesteld aan bezoekers van een opleidingscentrum.

2) Een **kantoor toestel** is gekoppeld aan een overheidsnetwerk en heeft slechts een beperkte verwerkingscapaciteit. Er wordt aanbevolen om geen lokale opslag te ondernemen van gegevens. Het toestel omvat enkel generieke functionaliteiten en zal dus enkel gebruikt worden voor administratieve toepassingen.

3) Een **gespecialiseerd toestel** is gekoppeld aan een overheidsnetwerk. Een belangrijk deel van de informatieverwerking vindt lokaal plaats. Zowel generieke als gespecialiseerde functionaliteiten zullen plaatsvinden op dit toestel (werkstation voor ontwikkelaars).

Maatregelen binnen de (mobiele) werkplek

Maatregelen tegen stroomstoring.

Als de computers gevoelig zijn voor het wegvallen van spanning en de continuïteit van de werkplek van essentieel belang is, kan een noodstroomvoorziening ingezet worden.

Maatregelen tegen diefstal.

Met behulp van kabels, sloten, bewakers, en dergelijke kunnen vaste werkplekken eenvoudig beschermd worden. Maatregelen voor kleine apparatuur is noodzakelijker aangezien deze eenvoudiger te ontvreemden zijn (bv. een notebook of smartphone). Men moet de nodige aandacht besteden aan onbeheerd materiaal (bv door uit te loggen wanneer men niet actief is op het netwerk of apparaat). Cryptografie kan een handig hulpmiddel zijn om ongeautoriseerde toegang te verhinderen (zie document Cryptografie).

Omgaan met documenten

Ook het omgaan met documenten, binnen de (mobiele) werkplek, vereist de nodige maatregelen. Niet-publieke documenten moeten namelijk fysiek beschermd worden tegen ongeautoriseerd toegang. Volgende maatregelen worden voorgesteld:

- kritische documenten moeten na gebruik opgeborgen worden in een afsluitbare/ brandvrije kast;
- toepassen van het ‘clean desk’ en ‘clear screen’ principe;
- blanco formulieren en toegangsbadges moeten opgeborgen worden in een afsluitbare kast;
- men moet het meelezen van documenten door onbevoegden voorkomen, dit kan o.a. door het gebruik van een security screen filter op mobiele apparatuur.

Beveiliging van apparatuur

Wegens de informatie, opgeslagen in apparatuur, verdient de beveiliging hiervan de nodige aandacht. Er moet getracht worden om te voorkomen dat deze apparatuur beschadigd of vernietigd wordt. De beveiligingsmaatregelen hangen uiteraard af van de informatie die opgeslagen wordt op deze apparatuur.

Plaatsing van apparatuur

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en gelegenheid voor onbevoegde toegang zodanig wordt verminderd.

Tijdens de plaatsing van apparatuur in een ruimte moet rekening worden gehouden met volgende vereisten:

1) locatie van apparatuur;
    i. men dient rekening te houden met de aanwezigheid van vensters en verdieping, met het oog op mogelijk wateroverlast en inkijk

2) toegankelijkheid van apparatuur;
    i. kritische apparatuur mag niet aanwezig zijn in publieke ruimtes of in ruimtes waar niet-geautoriseerde medewerkers kunnen vertoeven)

3) plaatsing in afsluitbaar server rack;

4) alternatieve stroomvoorziening;
    i. via een (nood)stroomopwekking moet de elektriciteitsvoorziening kunnen worden gegarandeerd voor kritische apparatuur

5) beveiliging tegen onderbreking van nutsvoorzieningen;

6) afscherming van voedings- en telecom kabels

Behandelen van apparatuur

Tijdens het transport, uit dienst name of onderhoud van apparatuur moeten de nodige voorzorgsmaatregelen genomen worden, om diefstal of beschadiging te voorkomen. Dit geldt niet alleen voor servers en andere netwerkapparatuur, maar ook voor printers, Pc's en andere apparatuur. Volgende vereisten zijn van toepassing op apparatuur:

1) Onderhoud, verplaatsing of transport (buiten de organisatie) mag enkel gebeuren door bevoegd en getraind personeel en/of externe medewerkers.

2) Indien apparatuur uit dienst genomen wordt, hergebruikt of voor herstel buiten de organisatie gebracht wordt, moeten gevoelige gegevens verwijderd worden zodat ze niet meer kunnen gereconstrueerd worden. Men moet overgaan tot vernietiging of adequaat wissen van gegevens of apparatuur, gebaseerd op een risicobeoordeling. De gepaste maatregel voor het wissen van gegevens moet contractueel vastgelegd worden (bev. Leasing, Cloud computing)

3) Apparatuur moet worden onderhouden volgens de onderhoudsvoorschriften van de leverancier.

4) Apparatuur buiten de locaties moet worden beveiligd en gebruikers moeten maatregelen nemen om onbewaakte apparatuur te beschermen.

Link met andere maatregelen

Link met IAM als maatregel

Fysieke toegangsbeveiliging is complementair aan Identity Access Management, dit wordt uitgelegd in het document IAM.

Link met logging als maatregel

Fysieke beveiliging gaat meestal gepaard met logging. Het gaat hier bijvoorbeeld om:

- het bijhouden van bezoekersregistratie of een bezoekerslogboek;
- het bijhouden van een onderhoudslogboek.

Manuele logging vereist de nodige discipline om fouten te vermijden. Er heerst een groot risico op fouten, mede door de hoeveelheid van uitvoerders die erbij betrokken zijn.

Mitigerende maatregelen om manuele logboeken te beveiligen bestaan o.a. uit:

- fysieke toegangsbeveiliging d.m.v. afsluitbare/brandveilige kast;
- kopieën bijhouden van het logboek;
- inscannen en opslaan als pdf bestand;
- controle en 4-ogen principe.

Link met regionale en lokale brandbeveiligingseisen

De organisaties moet rekening houden met regionale en lokale brandbeveiligingseisen waaraan hun organisatie moet voldoen (bv. Seveso zone).

Link met functiescheiding

Er is een link tussen informatiebeveiliging en het scheiden van functies. Het scheiden van de maatregelen op basis van de functies volgt in lijn met de arbeidsverdeling van de organisatie. Elke functie heeft zijn eigen specifieke maatregelen, die zelfstandig moeten uitgevoerd worden.

Globaal gelden de volgende functiescheidingen:

- tussen uitvoerende en controlerende taken;
- tussen beleid en uitvoering;
- tussen fysieke beveiliging en levering/beveiliging van ICT.

Fysieke toegangsbeveiliging heeft als doel gebouwen en informatie te beschermen door ongeautoriseerde toegang te voorkomen en kent haar eigen functiescheiding:

- eigen medewerkers versus bezoekers;
    - alleen aan personen die geen deel uitmaken van de organisatie worden bezoekerspassen verstrekt
- extern onderhoudspersoneel;
    - deze maken geen deel uit van de eigen organisatie en dienen voorzien te zijn van een bezoekerspas of alternatief identificatiemiddel
- uitvoerend versus controlerend personeel.
    - uitvoerend personeel mag in principe geen controlerende taken uitvoeren (tenzij in het kader van zelfcontrole)

Handhaving

Zie Algemeen beleid voor informatieveiligheid.

Documentbeheer

Historiek

Datum	*Auteur*	*Versie*	*Omschrijving wijzigingen*
5/04/2019	BOSA	v.0.1	Eerste draft
16/04/2019	BOSA	v.0.2	Update na review door de FISP werkgroep
17/04/2019	BOSA	v.0.3	Update na review door de FISP werkgroep
21/11/2019	FISP workgroup	V.1.0	Publieke verspreiding

Goedkeuringen

Datum	*Approver(s)*	*Versie*
21/11/2019	FISP FISP workgroup	V.1.0

Bronnen

Dit document werd samengesteld met behulp van de volgende bronnen:

- Fysieke controlemaatregelen – Informatieclassificatie Vlaamse overheid
- BIBOSA – 11 – Fysieke Beveiliging en beveiliging van de omgeving
- IEC27001/2
- Minimale normen, KSZ
- Baseline Security Guidlines, CCB

Link met een ander beleid

Afhankelijkheid van interne documenten

Ref	*Titel*
FISPDOC08	*Algemeen overzicht voor de informatieveiligheid op federaal niveau*
FISPDOC05	*Handleiding voor de beveiliging en het beheer van de identiteiten en de basistoegangen (IAM) en de geprivilegieerde toegangen (PAM)*
FISPDOC03	*Handleiding voor cryptografie*

Positionering van het beleid t.o.v. de ISO 27001-norm

Sectie	***Doelstellingen en referentiemaatregelen***	*In relatie (X = Ja*
4	*Context van de organisatie*	
5	*Leiderschap*	
6	*Planning*	*x*
7	*Ondersteuning*	
8	*Operatie*	*x*
9	*Evaluatie van de prestaties*	
10	*Verbeteringen*	

Positionering van het beleid t.o.v. de ISO 27002-norm

Sectie	**Doelstellingen en referentiemaatregelen**	In Relatie *(X = Ja)*	Doelstellingen / Maatregelen *(Detail)*
A5	*Informatiebeveiligingsbeleid*		
A6	*Organisatie van informatiebeveiliging*		
A7	*Human Resources Veiligheid*		
A8	*Asset Management*		
A9	*Toegangscontrole*		
A10	*Geheimschrift*		
A11	*Fysieke en ecologische veiligheid*	*x*	*11.1 + 11.2*
A12	*Operationele veiligheid*		
A13	*Beveiliging van communicatie*		
A14	*Aankoop, ontwikkeling en onderhoud van informatiesystemen*		
A15	*Relaties met leveranciers*		
A16	*Beheer van informatiebeveiligingsincidenten*		

Sectie	**Doelstellingen en referentiemaatregelen**	In Relatie *(X = Ja)*	Doelstellingen / Maatregelen *(Detail)*
A17	*Informatiebeveiliging in Business Continuity Management*		
A18	*Conformiteit*		