



CBR beleid Fysieke beveiliging

Versie controle
Inleiding
Doel van de Policy
Bereik van de policy
Definities
Verantwoordelijkheden
Uitgangspunten
Bedrijfspannen
Minimumrequirements
Classificatie
Nieuwe CBR-panden
Zichtbaarheid en identificatie
Cameratoezicht
Bedrijfsmiddelen
Maatregelen
Houderschap
Uitgifte en inname
Incidentrapportage, registratie, maatregelen
Uitgaven

Details van uitgifte

Gepubliceerd door
CBR Corporate security

Titel	Versie	Doelgroep
Fysieke beveiliging	1.1.19	Geheel CBR (intern en extern)
Auteur	Origineel goedgekeurd door	Geldig tot
Tjitse van den Bos	Security Board	1 januari 2021,
CSO		tenzij eerder gewijzigd.
Status en laatste revisie	Goedgekeurd voor	Locatie van het
Definitief 1.2.19	Implementatie	document
19-01-2019	SB 24-01-2019	Communicatie Studio

Samenvatting

Het beleid Fysieke beveiliging is een verdere uitwerking van het algemene beveiligingsbeleid en maakt deel uit van het raamwerk waarin het Beveiligingsbeleid van het CBR in wordt vastgesteld.

Versie controle

Versie	Laatste revisie	Editor	Veranderingen/ Commentaar
0.1		TvdB	
1.0	17-11-2016	TvdB	Input Security Board verwerkt
1.1	19-06-2018	TvdB	Vervaldatum en huisstijl aangepast, GoG toegevoegd bij incidentrapportage.
1.2.19	19-01-2019	TvdB	Indeling 1.3; 2.2; 3.3 gewijzigd. Hs 4 uitgebreid met Maatregelen.

NB:

Een papieren kopie van dit document is mogelijk niet de laatste versie. Controleer of dit de juiste versie is op de plek waar deze digitaal staat vermeld. (intranet: Organisatie: Security & Privacy)

Inhoudsopgave

Versie controle	2
1 Inleiding	4
1.1 Doel van de Policy	4
1.2 Bereik van de policy	4
1.3 Definities	4
1.4 Verantwoordelijkheden	4
1.5 Uitgangspunten	4
2 Bedrijfspannen	6
2.1 Minimumrequirements	6
2.2 Classificatie	6
2.3 Nieuwe CBR-panden	6
2.4 Zichtbaarheid en identificatie	6
2.5 Cameratoezicht	6
3 Bedrijfsmiddelen	7
3.1 Maatregelen	7
3.2 Houderschap	7
3.3 Uitgifte en inname	7
4 Incidentrapportage, registratie, maatregelen	7
5 Uitgaven	7

Versie controle
Inleiding
Doel van de Policy
Bereik van de policy
Definities
Verantwoordelijkheden
Uitgangspunten
Bedrijfspannen
Minimumrequirements
Classificatie
Nieuwe CBR-panden
Zichtbaarheid en identificatie
Cameratoezicht
Bedrijfsmiddelen
Maatregelen
Houderschap
Uitgifte en inname
Incidentrapportage, registratie, maatregelen
Uitgaven

1 Inleiding

Deze policy maakt deel uit van het security raamwerk van het CBR. Deze policy is een aanvulling op het Algemene Beveiligingsbeleid en Corporate Security Policy en gaat meer specifiek in op de eisen die gesteld worden aan fysieke beveiliging.

1.1 Doel van de Policy

Het doel van fysieke beveiliging is om medewerkers, leveranciers en bezoekers van het CBR te beschermen tegen inbreuk op de fysieke integriteit en vrijheid van beweging en werkzaamheden door standaarden voor een passend niveau van veiligheid te bieden. De beschreven securitymaatregelen dienen om bedreiging van panden en middelen in een vroegtijdig stadium te detecteren, bewijzen vast te leggen alsook om de veroorzakers van deze bedreigingen te kunnen identificeren.

1.2 Bereik van de policy

Dit beleidsdocument is van toepassing op alle medewerkers, leveranciers en bezoekers van het CBR.

1.3 Definities

Fysieke beveiliging kan worden uiteengezet in bescherming van panden en bescherming van eigendommen/assets (voor bescherming van personen: zie Personeels- en eventbeveiligingsbeleid).

Onder panden wordt verstaan het fysieke pand waarin werkzaamheden van het CBR worden uitgevoerd, de hierbinnen gevestigde ruimten en de omliggende terreinen met de zich hierop bevindende opstallen.

Onder eigendommen wordt verstaan alle roerende zaken toebehorend aan het CBR, haar medewerkers, leveranciers en bezoekers.

Bescherming van ICT-hardware, zoals servers en computerruimten, is vastgelegd in het ICT securitybeleid.

1.4 Verantwoordelijkheden

Het Security management, Facilitaire Zaken, medewerkers en managers zijn verantwoordelijk voor het beschermen van panden en eigendommen.

Het Security management is overall verantwoordelijk en beschrijft verantwoordelijkheden en rollen van betrokken partijen in bescherming van goederen en eigendommen in nader beleid.

Versie controle
Inleiding
Doel van de Policy
Bereik van de policy
Definities
Verantwoordelijkheden
Uitgangspunten
Bedrijfspannen
Minimumrequirements
Classificatie
Nieuwe CBR-panden
Zichtbaarheid en identificatie
Cameratoezicht
Bedrijfsmiddelen
Maatregelen
Houderschap
Uitgifte en inname
Incidentrapportage, registratie, maatregelen
Uitgaven

Het security management ontwikkelt securitymaatregelen en coördineert deze samen met de betreffende afdelingen, in het bijzonder Facilitaire zaken en de gebruiker. Security ondersteunt de betreffende afdelingen die verantwoordelijk zijn voor de implementatie van maatregelen. Security monitort alle maatregelen binnen fysieke security. Securitymaatregelen kunnen onderdeel worden van een audit.

De gebruiker van een pand (afdeling) is primair verantwoordelijk voor implementatie en monitoren van de relevante securitymaatregelen. Hieronder valt, onder andere, de verplichting om zich in panden correct te gedragen, het pand op bedoelde wijze te betreden en te verlaten, en om in lijn met brandveiligheidsvoorschriften te handelen.

De gebruiker van een pand is primair verantwoordelijk voor het beschermen van zijn of haar persoonlijke en bedrijfseigendommen.

1.5 Uitgangspunten

De volgende uitgangspunten gelden voor fysieke beveiliging:

Risicogebaseerde aanpak

Maatregelen om panden en eigendommen te beschermen zijn gebaseerd op een, bij voorkeur schriftelijk vastgelegde, risicoanalyse, waarin de betreffende dreigingen, impact en mogelijke maatregelen worden afgewogen in kosten en effectiviteit van de maatregelen.

Wanneer een dreigingsanalyse geen relevante risico's vaststelt hoeven geen maatregelen genomen te worden. Voor het uitvoeren van dreigingsanalyse is het noodzakelijk om over alle beschikbare en relevante informatie te beschikken.

Kosteneffectiviteit

De kosten van een securitymaatregel zullen altijd redelijk zijn en in verhouding staan tot het te beschermen belang/pand eigendom.

Versie controle
Inleiding
Doel van de Policy
Bereik van de policy
Definities
Verantwoordelijkheden
Uitgangspunten
Bedrijfspanden
Minimumrequirements
Classificatie
Nieuwe CBR-panden
Zichtbaarheid en identificatie
Cameratoezicht
Bedrijfsmiddelen
Maatregelen
Houderschap
Uitgifte en inname
Incidentrapportage, registratie, maatregelen
Uitgaven

2 Bedrijfspanden

2.1 Minimumrequirements

Voor beveiliging van panden en ruimten worden door Facilitaire zaken minimumrequirements vastgesteld voor braakwerendheid, sloten, ruiten alarmsystemen etc. Hierbij wordt rekening gehouden met de in het pand aanwezige informatie en eigendommen en de kosteneffectiviteit van de maatregelen.

2.2 Classificatie

CBR gebruikt panden met diverse inrichtingen en voor diverse doelen. Afhankelijk van het type gebruiker kunnen zich in het pand kritieke processen of gevoelige informatie bevinden.

Ruimten waarin zich kritieke ICT structuur of gevoelige informatie bevinden, worden naar gelang hun gevoeligheid geclassificeerd als ruimten met beperkte toegang. Dit houdt in dat de ruimte slechts toegankelijk is voor medewerkers zie voor het uitoefenen van hun functie toegang behoeven. De classificatie van ruimten en toegangsautorisaties wordt verder uitgewerkt in het ICT-beleid en Toegangsbeleid.

2.3 Nieuwe CBR-panden

Voor ieder pand dat door CBR in gebruik wordt genomen, wordt door Security een scan gemaakt van de risico's die het pand met zich meebrengt en de wijze waarop deze risico's kunnen worden gemitigeerd. De maatregelen die uit deze analyse voortkomen kunnen wenselijk danwel noodzakelijk van aard zijn. Uitvoering van deze maatregelen geschiedt primair door Facilitaire zaken en secundair door de gebruiker van het pand.

2.4 Zichtbaarheid en identificatie

Op terreinen en in panden van het CBR zijn medewerkers als zodanig herkenbaar en visueel te onderscheiden van bezoekers en kandidaten. Regels omtrent zichtbaarheid en identificatie van medewerkers en bezoekers worden nader vastgelegd in een Toegangsbeleid.

2.5 Cameratoezicht

Ten behoeve van preventief toezicht en het vastleggen en opsporen van strafbare feiten wordt gebruikt gemaakt van cameratoezicht op terreinen van het CBR. De uitgangspunten van cameratoezicht en de hieraan gekoppelde privacyregels wordt nader vastgelegd in het protocol Cameratoezicht.

Versie controle
Inleiding
Doel van de Policy
Bereik van de policy
Definities
Verantwoordelijkheden
Uitgangspunten
Bedrijfspanen
Minimumrequirements
Classificatie
Nieuwe CBR-panden
Zichtbaarheid en identificatie
Cameratoezicht
Bedrijfsmiddelen
Maatregelen
Houderschap
Uitgifte en inname
Incidentrapportage, registratie, maatregelen
Uitgaven

3 Bedrijfsmiddelen

3.1 Maatregelen

Maatregelen voor het beschermen van eigendommen zijn gericht op bescherming tegen beschadiging of verlies van eigendommen. Wanneer deze eigendommen gegevensdragers zijn, is het Informatiebeveiligingsbeleid van toepassing.

3.2 Houderschap

De persoon die eigendommen van het CBR in bruikleen heeft dient te waarborgen dat deze eigendommen niet onbeheerd worden gelaten en veilig worden opgeborgen en alle maatregelen te nemen die van een goed houder verwacht mogen worden.

3.3 Uitgifte en inname

Uitgifte en inname van bedrijfseigendommen die een aanzienlijke waarde vertegenwoordigen (o.a. laptops, gsm, tablet, bedrijfspas) wordt centraal geregistreerd.

4 Incidentrapportage, registratie, maatregelen

Security-incidenten, zoals grensoverschrijdend gedrag, inbraak, ongeautoriseerde toegang, diefstal etc. worden gemeld aan en geregistreerd door Security. Security maakt, in overleg met de betreffende afdelingen, centraal beleid en houdt toezicht op het uitvoeren van preventieve en repressieve maatregelen op basis van gemelde incidenten.

Security voorziet de Security Board periodiek van de betreffende incidentrapportages.

5 Uitgaven

Uitgaven voor bescherming van panden, terreinen en niet-ICT gerelateerde bedrijfsmiddelen, zoals cameratoezicht, bewakings- en toegangssystemen worden goedgekeurd door Facilitaire zaken.