Informatieclassificatie Vlaamse overheid (Vo-ICR)

Fysieke controlemaatregelen

Minimale maatregelen

Team Informatieveiligheid| Digitaal Vlaanderen

Dit is een document voor publiek gebruik

AGENTSCHAP
DIGITAAL VLAANDEREN
HAVENLAAN 88 BUS 60, 1000 BRUSSEL

Classificatie: Klasse 2

INHOUD VAN DIT DOCUMENT

Situering van het document

Dit document maakt deel uit van de begeleidende documentatie in context van het generieke informatieclassificatieraamwerk (ICR) van de Vlaamse overheid (Vo) op initiatief van het Stuurorgaan Vlaams Informatie- en ICT Beleid.

Doel van het document

Dit document beschrijft de kwaliteitseisen van de minimale maatregelen die moeten afgedwongen worden in het kader van de deelprocessen fysieke beveiliging. Deze kwaliteitseisen worden verbonden aan de informatieklassen zoals deze zijn beschreven in het ICR van de Vo.

Werkprincipe van het document

Het huidige document bestaat uit 3 delen. Eerst worden de minimale maatregelen besproken, alvorens in het tweede deel al de nodigde aanvullende informatie ter beschikking wordt gesteld. We sluiten af door de link met andere maatregelen toe te lichten.

De organisatie van de maatregelen in het kader van informatieclassificatie wordt beschreven in het document 'Vo informatieclassificatie – Organisatie - Informatieclassificatieraamwerk'.

Verspreiding van het document

Dit document is voornamelijk voor intern gebruik en bevat informatie die mag gedeeld worden met personen verbonden aan de Vo en zijn diensten leveranciers.

Het document mag gedeeld worden met derden onder de richtlijnen openbaarheid van bestuur van de Vlaamse regering.

Vrijwaring

Dit document geeft de huidige status en daaraan gerelateerde informatie binnen het project weer. Gelieve de auteur of de bevoegde project begeleiders te contacteren om zich ervan te vergewissen dat u de laatst gevalideerde versie van dit document in handen heeft.

Eigenaar

Voorzitter werkgroep informatieveiligheid | Digitaal Vlaanderen

security@vlaanderen.be

Classificatie

Dit document valt onder de vertrouwelijkheidsklasse 1 (Publiek) en mag toegankelijk zijn voor iedereen.

Dit document valt onder integriteitsklasse 2. De organisatie heeft **geen directe hinder** indien de informatie gewijzigd wordt door onbevoegden en de **dienstverlening blijft gegarandeerd**. Maar bijsturing van de criteria en/of maatregelen is aangewezen.

Historiek

	Datum	Auteur	Opmerkingen
v.0.1	9 april 2018	Kristel VAN AKEN	Eerste draft
v.0.2	29 juni 2018	Kristel VAN AKEN	Feedback Johan Smekens verwerkt + document aangevuld
v.0.3	3 juli	Johan SMEKENS	Review
v.0.4	21 augustus 2018	Kristel VAN AKEN	Feedback overleg 'kantoor 2023'
v.1.1	16 oktober 2018	Kristel VAN AKEN	Aanvulling maatregelen per klasse
v.1.2	18 december 2019	Kristel VAN AKEN	Feedback leespanel
v.1.3	16 April 2020	Kristel VAN AKEN	Versie gepubliceerd in pdf
v.1.4	2 oktober 2020	Kristel VAN AKEN	Integriteit toegevoegd
v.1.5	10 juni 2021	Kristel VAN AKEN	Beschikbaarheid toegevoegd
v.2.0	22 juli 2022	Kristel VAN AKEN	Verbeteren leesbaarheid Geen inhoudelijke wijzigingen
V2.1	17 oktober 2023	Nele LOWET	Update KSZ

Bronnen en verwijzingen

De inhoud van dit document werd samengesteld op basis van volgende documenten:

Documentverwijzingen:

- *Vo informatieclassificatie – Organisatie Informatieveiligheid* (PDF)
- *Vo Informatieclassificatie – Organisatie Informatieclassificatieraamwerk* (PDF)
- Kantoor 2023
- Kennisplatform NORA
- Vo Informatieclassificatie – Minimale maatregelen – (PDF):
  - *Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*
  - *Vo Informatieclassificatie - Minimale maatregelen – IAM*
  - *Vo Informatieclassificatie - Minimale maatregelen – netwerken*
- *Vo Informatieclassificatie – Overzicht baseline maatregelen* (XLS)

De laatste versies van deze documenten zijn te raadplegen op vlaanderen.be.

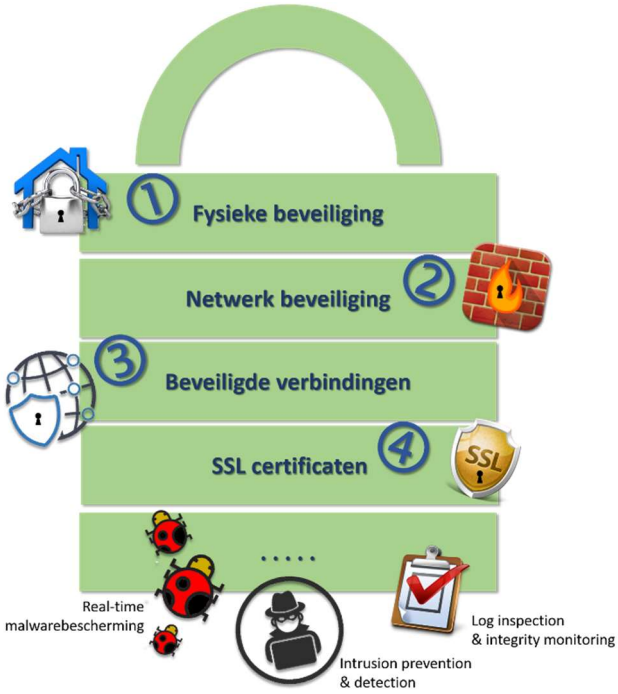
INHOUDSOPGAVE

INLEIDING

Bij de inrichting van een locatie, gebouwen en ruimtes is het van belang dat aandacht wordt besteed aan fysieke beveiliging. Dit is zeker het geval voor kritische ruimtes, zoals datacenters en ruimtes voor technische apparatuur.

Daarnaast mag ook de controle op de werkplek door middel van fysieke veiligheidsmaatregelen niet uit het oog verloren worden.

Volgende schema illustreert dat fysieke beveiliging samen met andere beveiligingsmaatregelen onderdeel uitmaken van een globale aanpak voor informatiebeveiliging:



Fysieke beveiliging omvat het geheel van maatregelen dat betrekking heeft op het voorkomen of beperken van schadelijke gevolgen van fysieke gebeurtenissen zoals verlies, vandalisme, inbraak, bliksem- of wateroverlast. De waarde van apparatuur en de gevoeligheid van gegevens vormen reden tot het nemen van maatregelen op het gebied fysieke beveiliging. Diefstal van apparatuur en gegevens geeft, naast materieel verlies, problemen voor de continuïteit van de gegevensverwerking.

Fysieke beveiliging omvat ook alle maatregelen op beveiliging tegen omgevingsfactoren, ontvallen van nutsvoorzieningen en natuurrampen door middel van:

- Fysieke toegangsbeveiliging;
- Beveiliging van gebouwen en locaties;
- Beveiliging van apparatuur;
- Beveiliging van de werkplek.

Fysieke beveiliging behoort vaak tot het domein van de facilitaire dienst of technische dienst.

1. MINIMALE MAATREGELEN

1.1 Minimale algemene maatregelen

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	**Publiek toegankelijke ruimtes** 〉 Eventueel controlerende maatregelen zoals camerabewaking
	**De gewone werkplek van de medewerkers** Alle maatregelen van Klasse 1 + 〉 Zonering op niveau organisatie. 〉 Aparte laad- en loszone. 〉 Toegang beperken d.m.v. sleutels (mechanisch of digitaal) of toegangsbadges. 〉 Individuele credentials voor medewerkers. 〉 Up-to-date inventaris van personeel en hun toegangsmodaliteiten 〉 Bezoekersregistratie. 〉 Zichtbaar dragen van identificatiemiddelen (badges, stickers bezoekers, …) 〉 Brandbeveiliging en –detectie. 〉 Automatische noodverlichting. 〉 Regels voor het maken van foto's of opnames (goedkeuring eigenaar). 〉 Verwijderen van informatie voor apparatuur wordt afgevoerd. 〉 Sensibilisering rond fysieke veiligheid van apparatuur: 〉 Actieve sessie na beëindiging afsluiten of vergrendelen 〉 Uitloggen toepassingen/netwerkdiensten 〉 Vergrendelen mobiele apparatuur 〉 Gebruikersapparatuur automatisch vergrendelen na time-out. 〉 Informatie op het scherm afschermen
	**De werkplek van medewerkers met toegang tot vertrouwelijke informatie** Alle maatregelen van Klasse 1 + Klasse 2 + 〉 Zonering op niveau functionele behoefte. 〉 Begeleiding van bezoekers. 〉 Jaarlijks nazicht inventaris personeel en hun toegangsmodaliteiten. 〉 Gemaakte foto's of opnames moeten door de eigenaar gecontroleerd worden. 〉 Toegankelijkheid van beeldschermen, printers, faxen, kopieerapparatuur, scanners, video/audio, … beperken. 〉 Bekabeling beveiligen tegen schade, afluisteren, vernietiging (bvb aparte kabelgoten, afgesloten kabelkasten, veilig opbergen reservemateriaal, …). 〉 Transport van apparatuur buiten de organisatie enkel door goedgekeurd personeel/firma's. 〉 Bewezen methodes gebruiken voor verwijderen van informatie. 〉 *Clear desk* en *clear screen* principe toepassen

	〉 Informatie op papier of verwijderbare media in afgesloten kast bewaren. 〉 Output printers, kopieerapparaten, faxen, ... onmiddellijk verwijderen.
	**De werkplek van medewerkers met toegang tot geheime informatie** Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + 〉 Testen of informatie verwijderd is vooraleer apparatuur wordt afgevoerd.
	**Datacenter** Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 + Klasse 4 + 〉 Aparte fysieke toegang, beveiligd d.m.v. toegangsbadges 〉 Bewaking van de toegangscontrole via camera's, bewakingspersoneel, … 〉 Beveiligen van kabels tegen vandalisme, beschadiging en afluisteren. 〉 Toegang door extern personeel (onderhoud, schoonmaken): 4-ogen principe toepassen. 〉 Automatische branddetectie met alarmfunctie. 〉 Gespecialiseerde blusapparatuur. 〉 Automatische detectie van water. 〉 Monitoring van temperatuur en vochtigheid. 〉 Alternatieve of back-up sites voorzien van gelijkwaardige beveiliging. 〉 Het maken van foto's of opnames verbieden. 〉 Verificatie van beveiligingsniveau en -mechanismen na onderhoud apparatuur 〉 Verwijderen van apparatuur: 4-ogen principe toepassen.

Integriteit

IC klasse	Minimale maatregelen
	〉 Eventueel controlerende maatregelen zoals camerabewaking

	Alle maatregelen van Klasse 1 +
	
	〉 Zonering op niveau organisatie.
	〉 Aparte laad- en loszone.
	〉 Toegang beperken d.m.v. sleutels (mechanisch of digitaal) of toegangsbadges.
	〉 Individuele credentials voor medewerkers.
	〉 Up-to-date inventaris van personeel en hun toegangsmodaliteiten
	〉 Bezoekersregistratie.
	〉 Zichtbaar dragen van identificatiemiddelen (badges, stickers bezoekers, …)
	〉 Brandbeveiliging en –detectie.
	〉 Automatische noodverlichting.
	〉 Verwijderen van informatie voor apparatuur wordt afgevoerd.
	〉 Sensibilisering rond fysieke veiligheid van apparatuur:
	  〉 Actieve sessie na beëindiging afsluiten of vergrendelen
	  〉 Uitloggen toepassingen/netwerkdiensten
	  〉 Vergrendelen mobiele apparatuur
	  〉 Gebruikersapparatuur automatisch vergrendelen na time-out.

	〉 Informatie op het scherm afschermen
	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 + Klasse 2 + 〉 Zonering op niveau functionele behoefte. 〉 Begeleiding van bezoekers. 〉 Jaarlijks nazicht inventaris personeel en hun toegangsmodaliteiten. 〉 Bekabeling beveiligen tegen schade, afluisteren, vernietiging (bvb aparte kabelgoten, afgesloten kabelkasten, veilig opbergen reservemateriaal, …). 〉 Transport van apparatuur buiten de organisatie enkel door goedgekeurd personeel/firma's.
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 / Klasse 4 + 〉 Aparte fysieke toegang, beveiligd d.m.v. toegangsbadges 〉 Bewaking van de toegangscontrole via camera's, bewakingspersoneel, … 〉 Beveiligen van kabels tegen vandalisme, beschadiging en afluisteren. 〉 Toegang door extern personeel (onderhoud, schoonmaken): 4-ogen principe toepassen. 〉 Automatische branddetectie met alarmfunctie. 〉 Gespecialiseerde blusapparatuur. 〉 Automatische detectie van water. 〉 Monitoring van temperatuur en vochtigheid. 〉 Alternatieve of back-up sites voorzien van gelijkwaardige beveiliging. 〉 Verificatie van beveiligingsniveau en -mechanismen na onderhoud apparatuur 〉 Verwijderen van apparatuur: 4-ogen principe toepassen.

Beschikbaarheid

IC klasse	Minimale maatregelen
	〉 Eventueel controlerende maatregelen zoals camerabewaking
	Alle maatregelen van Klasse 1 + 〉 Maatregelen om diefstal tegen te gaan: 〉 Zonering op niveau organisatie. 〉 Aparte laad- en loszone. 〉 Toegang beperken d.m.v. sleutels (mechanisch of digitaal) of toegangsbadges. 〉 Individuele credentials voor medewerkers. 〉 Up-to-date inventaris van personeel en hun toegangsmodaliteiten 〉 Bezoekersregistratie. 〉 Zichtbaar dragen van identificatiemiddelen (badges, stickers bezoekers, …) 〉 Brandbeveiliging en –detectie. 〉 Voldoende reservemateriaal en/of support/onderhoudscontracten voorzien.
 	Klasse 3 en Klasse 4 kennen dezelfde maatregelen: Alle maatregelen van Klasse 1 + Klasse 2 + 〉 Maatregelen om diefstal tegen te gaan: 〉 Zonering op niveau functionele behoefte. 〉 Begeleiding van bezoekers. 〉 Jaarlijks nazicht inventaris personeel en hun toegangsmodaliteiten. 〉 Bekabeling beveiligen tegen schade en vernietiging (bvb aparte kabelgoten, afgesloten kabelkasten, veilig opbergen reservemateriaal, …) 〉 24x7 support/onderhoudscontracten voorzien.
	Alle maatregelen van Klasse 1 + Klasse 2 + Klasse 3 / Klasse 4 + 〉 Maatregelen om diefstal tegen te gaan: 〉 Aparte fysieke toegang, beveiligd d.m.v. toegangsbadges 〉 Bewaking van de toegangscontrole via camera's, bewakingspersoneel, … 〉 Beveiligen van kabels tegen vandalisme, beschadiging en vernietiging. 〉 Toegang door extern personeel (onderhoud, schoonmaken): 4-ogen principe toepassen. 〉 Automatische branddetectie met alarmfunctie. 〉 Gespecialiseerde blusapparatuur. 〉 Automatische detectie van water. 〉 Monitoring van temperatuur en vochtigheid. 〉 Alternatieve of back-up sites voorzien van gelijkwaardige beveiliging.

1.2 Minimale specifieke (GDPR) maatregelen

De minimale algemene fysieke maatregelen moeten toegepast worden: per klasse zijn de overeenkomende maatregelen van toepassing.

Er zijn geen minimale specifieke maatregelen voor GDPR fysieke beveiliging

1.3 Minimale specifieke (NISII) maatregelen

In afwachting van de goedkeuringen omtrent NISII is er in dit document alvast de nodige ruimte voorzien voor toekomstige minimale specifieke NISII maatregelen.

1.4 Minimale specifieke (KSZ) maatregelen

Volgens de Minimale Normen van de Kruispuntbank Sociale Zekerheid moeten volgende maatregelen in het kader van fysieke maatregelen toegepast worden:

Beschikbaarheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Een beleidslijn uitwerken waarbij wordt aangegeven dat de medewerking van alle medewerkers van essentieel belang is voor de informatieveiligheid en de privacy. Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen of tot documenten (Ref. KSZ 5.4.2 a). 〉 Elke organisatie moet zich ervan vergewissen dat de dragers van de persoonsgegevens en de informaticasystemen die deze gegevens verwerken10 in geïdentificeerde en beveiligde lokalen geplaatst worden, overeenkomstig hun indeling. Deze lokalen zijn enkel toegankelijk voor de gemachtigde personen en enkel tijdens de uren die voor hun functie gerechtvaardigd zijn (Ref. KSZ 5.5.3). 〉 Elke organisatie moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren (Ref. KSZ 5.8.1). 〉 Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritieke informatie en ICT voorzieningen bevinden (Ref. KSZ 5.8.1 a.). 〉 Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten (Ref. KSZ 5.8.1 b.). 〉 Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 c.). 〉 Elke organisatie moet maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade (Ref. KSZ 5.8.1 d.). 〉 Er moeten fysieke bescherming en richtlijnen voor werken in beveiligde ruimten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 e.). 〉 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 en/of ICT voorzieningen, om onbevoegde toegang te voorkomen (Ref. KSZ 5.8.1 f.). 〉 Elke organisatie moet maatregelen treffen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten (Ref. KSZ 5.8.2). 〉 Kritieke apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd (Ref. KSZ 5.8.2 a.).

	〉 Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, moeten tegen interceptie of beschadiging worden beschermd (Ref. KSZ 5.8.2 c.). 〉 Kritieke apparatuur moet op correcte wijze worden onderhouden, zodat deze voortdurend beschikbaar is en in goede staat verkeert (Ref. KSZ 5.8.2 d.). 〉 Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder voorafgaande toestemming van de locatie worden meegenomen (Ref. KSZ 5.8.2 e.). 〉 Apparatuur buiten de locaties moet worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie 〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 f.). 〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 h.). 〉 Bij het gebruik van vercijfering als preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager: ○ De encryptiesleutels nooit aanbrengen in een duidelijke vorm op de drager zelf. ○ De vercijfering moet betrekking hebben op logische volumes in hun geheel (in plaats van op bestanden of individuele repertoria). ○ De vercijfering dient als aanvulling op de toepasbare organisatorische en procedurele maatregelen die erop gericht zijn om misbruiken tegen te gaan (Ref. KSZ 5.8.3 a.). 〉 Bij hergebruik van de informatiedrager deze opnieuw gebruiken in een minstens vergelijkbaar dataclassificatieniveau (Ref. KSZ 5.8.3 b.). 〉 Een risico-beoordeling uitvoeren om de gepaste methode te bepalen voor het wissen van een informatiedrager (Ref. KSZ 5.8.3 c.). 〉 De gepaste maatregelen voor het wissen van gegevens contractueel vastleggen wanneer: ○ de organisatie informatiedragers gebruikt die geen eigendom zijn (bijvoorbeeld in het kader van leasing of disaster recovery) ○ de organisatie de technologie niet beheerst voor toegang tot alle niveaus van de informatiedrager (bijvoorbeeld in het kader van cloud computing) (Ref. KSZ 5.8.3 e). 〉 Elke organisatie moet over een alternatieve stroomvoorziening beschikken om de verwachte dienstverlening te waarborgen. Kritieke apparatuur moet worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen (Ref. KSZ 5.8.2 b.).

Integriteit

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Een beleidslijn uitwerken waarbij wordt aangegeven dat de medewerking van alle medewerkers van essentieel belang is voor de informatieveiligheid en de privacy.

   	Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen of tot documenten Ref. KSZ 5.4.2 a). 〉 Elke organisatie moet zich ervan vergewissen dat de dragers van de persoonsgegevens en de informaticasystemen die deze gegevens verwerken10 in geïdentificeerde en beveiligde lokalen geplaatst worden, overeenkomstig hun indeling. Deze lokalen zijn enkel toegankelijk voor de gemachtigde personen en enkel tijdens de uren die voor hun functie gerechtvaardigd zijn (Ref. KSZ 5.5.3). 〉 Elke organisatie moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren (Ref. KSZ 5.8.1). 〉 Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritieke informatie en ICT voorzieningen bevinden (Ref. KSZ 5.8.1 a.). 〉 Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten (Ref. KSZ 5.8.1 b.). 〉 Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 c.). 〉 Elke organisatie moet maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade (Ref. KSZ 5.8.1 d.). 〉 Er moeten fysieke bescherming en richtlijnen voor werken in beveiligde ruimten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 e.). 〉 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 en/of ICT voorzieningen, om onbevoegde toegang te voorkomen (Ref. KSZ 5.8.1 f.). 〉 Elke organisatie moet maatregelen treffen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten (Ref. KSZ 5.8.2). 〉 Kritieke apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd (Ref. KSZ 5.8.2 a.). 〉 Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, moeten tegen interceptie of beschadiging worden beschermd (Ref. KSZ 5.8.2 c.). 〉 Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder voorafgaande toestemming van de locatie worden meegenomen (Ref. KSZ 5.8.2 e.). 〉 Apparatuur buiten de locaties moet worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie 〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 f.).

	〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 h.). 〉 Bij het gebruik van vercijfering als preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager: ○ De encryptiesleutels nooit aanbrengen in een duidelijke vorm op de drager zelf. ○ De vercijfering moet betrekking hebben op logische volumes in hun geheel (in plaats van op bestanden of individuele repertoria). ○ De vercijfering dient als aanvulling op de toepasbare organisatorische en procedurele maatregelen die erop gericht zijn om misbruiken tegen te gaan (Ref. KSZ 5.8.3 a.). 〉 Bij hergebruik van de informatiedrager deze opnieuw gebruiken in een minstens vergelijkbaar dataclassificatieniveau (Ref. KSZ 5.8.3 b.). 〉 Een risico-beoordeling uitvoeren om de gepaste methode te bepalen voor het wissen van een informatiedrager (Ref. KSZ 5.8.3 c.). 〉 De gepaste maatregelen voor het wissen van gegevens contractueel vastleggen wanneer: ○ de organisatie informatiedragers gebruikt die geen eigendom zijn (bijvoorbeeld in het kader van leasing of disaster recovery) ○ de organisatie de technologie niet beheerst voor toegang tot alle niveaus van de informatiedrager (bijvoorbeeld in het kader van cloud computing) (Ref. KSZ 5.8.3 e.).

Vertrouwelijkheid

IC klasse	Minimale maatregelen
	Klasse 1 t/m Klasse 5 kennen dezelfde maatregelen: 〉 Een beleidslijn uitwerken waarbij wordt aangegeven dat de medewerking van alle medewerkers van essentieel belang is voor de informatieveiligheid en de privacy. Elke medewerker speelt een belangrijke rol in het vermijden van ongeoorloofde toegang tot gevoelige informatie. Dit geldt zowel voor de toegangen tot de informatiesystemen en toepassingen als voor de fysieke toegang tot lokalen of tot documenten Ref. KSZ 5.4.2 a). 〉 Elke organisatie moet zich ervan vergewissen dat de dragers van de persoonsgegevens en de informaticasystemen die deze gegevens verwerken10 in geïdentificeerde en beveiligde lokalen geplaatst worden, overeenkomstig hun indeling. Deze lokalen zijn enkel toegankelijk voor de gemachtigde personen en enkel tijdens de uren die voor hun functie gerechtvaardigd zijn (Ref. KSZ 5.5.3). 〉 Elke organisatie moet de toegang tot de gebouwen en lokalen beperken tot de geautoriseerde personen en een controle erop verrichten zowel tijdens als buiten de werkuren (Ref. KSZ 5.8.1). 〉 Er moeten toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) worden aangebracht om ruimten te beschermen waar zich gevoelige of kritieke informatie en ICT voorzieningen bevinden (Ref. KSZ 5.8.1 a.).

	〉 Privaat toegankelijke zones van een gebouw en de beveiligde ruimten moeten worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten (Ref. KSZ 5.8.1 b.). 〉 Er moet fysieke beveiliging van kantoren, ruimten en faciliteiten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 c.). 〉 Elke organisatie moet maatregelen treffen m.b.t. de preventie, de bescherming, de detectie, het blussen en de interventie in geval van brand, inbraak of waterschade (Ref. KSZ 5.8.1 d.). 〉 Er moeten fysieke bescherming en richtlijnen voor werken in beveiligde ruimten worden ontworpen en gerealiseerd (Ref. KSZ 5.8.1 e.). 〉 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 en/of ICT voorzieningen, om onbevoegde toegang te voorkomen (Ref. KSZ 5.8.1 f.). 〉 Elke organisatie moet maatregelen treffen ter voorkoming van verlies, schade, diefstal of compromitteren van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten (Ref. KSZ 5.8.2). 〉 Kritieke apparatuur moet zo worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang worden verminderd (Ref. KSZ 5.8.2 a.). 〉 Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, moeten tegen interceptie of beschadiging worden beschermd (Ref. KSZ 5.8.2 c.). 〉 Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder voorafgaande toestemming van de locatie worden meegenomen (Ref. KSZ 5.8.2 e.). 〉 Apparatuur buiten de locaties moet worden beveiligd, waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie 〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 f.). 〉 Gebruikers moeten zeker stellen dat onbewaakte apparatuur gepast beschermd wordt (Ref. KSZ 5.8.2 h.). 〉 Bij het gebruik van vercijfering als preventieve basismaatregel in geval van diefstal, misbruik of verlies van de informatiedrager: ○ De encryptiesleutels nooit aanbrengen in een duidelijke vorm op de drager zelf. ○ De vercijfering moet betrekking hebben op logische volumes in hun geheel (in plaats van op bestanden of individuele repertoria). ○ De vercijfering dient als aanvulling op de toepasbare organisatorische en procedurele maatregelen die erop gericht zijn om misbruiken tegen te gaan (Ref. KSZ 5.8.3 a.). 〉 Bij hergebruik van de informatiedrager deze opnieuw gebruiken in een minstens vergelijkbaar dataclassificatieniveau (Ref. KSZ 5.8.3 b.). 〉 Een risico-beoordeling uitvoeren om de gepaste methode te bepalen voor het wissen van een informatiedrager (Ref. KSZ 5.8.3 c.). 〉 De gepaste maatregelen voor het wissen van gegevens contractueel vastleggen wanneer:

	○ de organisatie informatiedragers gebruikt die geen eigendom zijn (bijvoorbeeld in het kader van leasing of disaster recovery) ○ de organisatie de technologie niet beheerst voor toegang tot alle niveaus van de informatiedrager (bijvoorbeeld in het kader van cloud computing) (Ref. KSZ 5.8.3 e). 〉 Elke organisatie moet de nodige maatregelen treffen opdat alle gegevens op opslagmedia gewist of ontoegankelijk gemaakt worden vóór verwijdering of hergebruik (Ref. KSZ 5.8.2 g.) 〉 Bij een voor de organisatie niet aanvaardbaar residuele risico van het terugvinden van de gegevens na het wissen, de informatiedrager fysiek vernietigen, zelfs als het residuele risico hypothetisch is (Ref. KSZ 5.8.3 d.).

2 AANVULLENDE INFORMATIE OVER DE MAATREGELEN

2.1 Fysieke locatie

Zonering

De classificatie van informatie leidt tot een fysieke opsplitsing van de locaties waar deze informatie verwerkt wordt. Door middel van zonering kan beveiliging praktisch gerealiseerd worden.

Voor zonering gelden volgende eisen, ingesteld afhankelijk van de informatieklasse toepasbaar op de bedoelde locatie:

- Personeel, bezoekers en leveranciers mogen uitsluitend toegang hebben of krijgen tot die zones waar dat omwille van hun werkzaamheden noodzakelijk is.
- De zones moeten doelmatig van elkaar te zijn gescheiden en er mag geen ongeautoriseerde toegang worden verkregen.
- Illegaal gebruik van een toegang (zoals door ‘meelopen’) naar kritische zones moet worden voorkomen of gedetecteerd.
- De apparatuur voor toegangscontrole moet zijn voorzien van een noodstroomvoorziening.
- Gescheiden ingangen voor personen en goederen (Aparte laad- en loszones)
- De maatregelen voor zonering (hekken, deuren), moeten voorzien zijn van de nodige controle- en monitoring mechanismen

- Detectie openstaande deuren
- Klem beveiliging automatische deuren
- Camerabewaking
- Signalisatie problemen (brand, wateroverlast)
- Inbraak beveiliging

- Ingeval van stroomonderbreking moeten de instellingen zodanig zijn dat de veiligheid van personen gegarandeerd blijft (vb. automatisch openen na stroomuitval).
- Er moeten incidentprocessen geïmplementeerd worden ter ondersteuning van de aanwezige personen

- Personeel en bezoekers
- Gebouw verantwoordelijken
- Baliepersoneel
- Bewakingsagenten

- Oproepen nooddiensten
- Enz.

Publieke, semipublieke en niet-publieke zone

Aansluitend op de onderverdeling in zones gedefinieerd in document kantoor 2023 worden 3 zones geïdentificeerd:

- Publieke zone: door haar open karakter kan (een entiteit van) de Vo geen of onvoldoende fysieke controle uitoefenen in deze zone om het gewenste veiligheidsniveau voor alle behalve publieke informatieverwerking te garanderen. Vanuit het standpunt van de organisatie is de werkplek thuis een publieke zone.
- Semipublieke zone: door haar semi-open karakter kan (een entiteit van) de Vo onvoldoende fysieke controle uitoefenen in deze zone om het gewenste veiligheidsniveau van sommige informatieverwerking te garanderen.
- Niet-publieke of private zone: dit is een Vo gecontroleerde zone. Afhankelijk van de klasse van de informatie die verwerkt wordt, worden organisatorische en technische maatregelen opgelegd om de fysieke veiligheid van de verwerkte informatie te borgen.

Fysieke toegangscontrole

Aangezien de Vo als overheidsinstantie een open instelling is met mogelijk grote circulatie van personen en sommige gebouwen een publieke functie hebben is een strikt beperken van toegankelijkheid niet overal mogelijk. Om de complexe gebruikersstroom op een veilige en gebruiksvriendelijke manier te organiseren worden volgende controlemaatregelen voorgesteld:

- Door middel van sleutels (mechanisch of digitaal), beheerd via een strikt sleutelplan;
- Door middel van persoonlijke toegangsbadges (inclusief tijdelijke toegangsbadges voor bezoekers).

Voor toegangscontrole gelden de volgende eisen:

- Verplichting voor werknemers tot identificatie. De toegangsbadges zijn persoonsgebonden. Blanco toegangsbadges of niet toegewezen badges moeten veilig opgeborgen worden.
- Bezoekers voor niet-publieke ruimtes 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.

- Bezoekers voor niet-publieke ruimtes moeten geregistreerd worden, vb. digitaal of door invullen van een bezoekerslog.
- Schoonmaak- en onderhoudspersoneel mag alleen in kritische zones werken onder permanent toezicht van medewerkers.
- Bewaking van toegangscontrole door middel van camerabewaking en/of bewakingspersoneel.

Beveiliging van gebouwen en locaties

Voor de bouwkundige infrastructuur worden de nodige vereisten gesteld zodat ze voldoende weerstand bieden aan omgevingsbedreigingen, het ontvallen van nutsvoorzieningen en natuurrampen.

Algemeen

Ruimtes moeten voldoen aan volgende vereisten:

- Weerstand aan calamiteiten (brand, blikseminslag, storm, hagel, overstroming/waterlekken, aardschok);
- Wand-, vloer- en plafondconstructies voldoen aan brandwerendheidseisen;
- Afwerking (stof, brand, rook);
- Diverse vluchtwegen;
- Externe elektriciteitstoevoer met voeding vanaf twee zijden;
- Arbeidsomstandigheden (licht, geluid, lucht);
- Maatregelen tegen schade door onder- of overspanning (onder andere bij bliksem);
- Overige wettelijke eisen of interne richtlijnen.

Voor het oplossen van technische storingen en het bieden van informatie over de infrastructuur moet er actuele documentatie over de bouwkundige voorzieningen beschikbaar zijn bij de beheerder van het gebouw.

Interne elektriciteitsvoorziening

Voor kritische ruimtes moet een no-break-installatie zijn geïnstalleerd met een capaciteit die voldoende is voor het (tijdelijk) voortzetten van de meest kritische bedrijfsprocessen.

De no-break-installatie moet minstens jaarlijks op goed functioneren worden getest en volgens de voorschriften worden onderhouden.

Telecommunicatie-infrastructuur

De interne (tele)communicatiebekabeling en -verdeelpunten moeten:

- Onbereikbaar zijn voor onbevoegden (zonering);
- Ruim bemeten en gespreid zijn;
- Afgeschermd zijn van voedingskabels, bliksemafleiders, TL-buizen, spoelen, etc.

Een UPS zorgt voor een tijdelijke no-break van de verschillende platformen.

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

Klimaatbeheersing

De luchtbehandeling van ruimtes met kritische apparatuur moet onafhankelijk zijn van de overige ruimtes, en het gevaar van aanzuiging van gevaarlijke stoffen moet beperkt zijn.

Er moet een mogelijkheid zijn om bij alarmering de luchtventilatie handmatig ‘UIT’ te schakelen.

Brandbeveiliging

Voor brandbeveiliging gelden een aantal vereisten rond preventie, detectie en bestrijding.

Preventieve voorzieningen

Bij de bouw en inrichting van kritische ruimtes moeten de toegepaste materialen zodanig gekozen worden dat ze brand- en rookontwikkeling beperken. Er moet aandacht geschonken worden aan brandwerende scheidingen. Dit geldt ook voor de aansluitingen van wanden en plafonds, doorvoer van luchtkanalen, elektriciteit- en andere leidingen, bijvoorbeeld door rookdicht sluitende brandkleppen.

De bliksemafleiderinstallatie moet zodanig worden geïnstalleerd dat schade door blikseminslag zoveel mogelijk wordt voorkomen.

Er is een wettelijk ingericht rookverbod in alle gebouwen van de Vo; er is een rookverbod in alle kritische (data) ruimtes.

Branddetectie en –signalering

Er moet detectieapparatuur en automatische (en handmatige) brandmelders aanwezig zijn in de kritische ruimtes (tevens onder verhoogde vloeren, boven verlaagde plafonds etc.) en in ruimtes met hoge brandveiligheidseisen. Regelmatig moet controle plaatsvinden op de werking van de detectieapparatuur. De detectieapparatuur moet voorzien zijn van een eigen noodstroomvoorziening.

Brandbestrijding

Er moeten instructies zijn die aangeven hoe te handelen in geval van brand waarin aandacht wordt besteed aan:

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

De kritische ruimtes moeten zijn voorzien van (een) automatische blusinstallatie(s). Hierbij moet een handmatige mogelijkheid te bestaan om deze uit te zetten. De blusinstallatie moet aangepast zijn aan de apparatuur en de mogelijke aanwezigheid van medewerkers en/of bezoekers.

Waterschade

Er mogen in de kritische ruimtes (wanden, vloer en plafond) geen leidingen aanwezig zijn voor het transport van water (vloeistoffen in het algemeen). In de directe omgeving van kritische apparatuur moeten vochtdetectors aanwezig zijn met automatische detectie en alarmering.

Opmerking: er moet uitzondering gemaakt worden voor brandblusinstallaties.

2.1.1 Beveiliging van apparatuur

Apparatuur moet zodanig geplaatst worden dat het beschermd wordt tegen beschadiging of vernietiging. Indien apparatuur verhuisd moet worden en/of getransporteerd, moeten de nodige voorzorgsmaatregelen genomen worden om diefstal of beschadiging tijdens transport te voorkomen.

Er moet ook aandacht worden besteed aan het verwijderen van apparatuur voor reparatie of uit dienst name. Dit geldt niet alleen voor servers en andere netwerkapparatuur, maar ook voor printers, PC's en andere apparatuur, afhankelijk van de klasse informatie die verwerkt wordt.

Plaatsing van apparatuur

Bij het plaatsen van apparatuur in een ruimte moet rekening worden gehouden met volgende vereisten:

- Locatie van apparatuur (aanwezigheid van vensters, verdieping met het oog op mogelijk wateroverlast en inkijk);
- Toegankelijkheid van apparatuur: kritische apparatuur mag niet in publieke ruimtes of in ruimtes waar niet-geautoriseerde medewerkers kunnen vertoeven;
- Plaatsing van apparatuur: in beveiligde ruimtes, op afstand van mogelijk wateroverlast (airco, kranen);
- Plaatsing in afsluitbaar server rack;
- Alternatieve stroomvoorziening: via een (nood)stroomopwekking moet de elektriciteitsvoorziening kunnen worden gegarandeerd (ook qua kwaliteit, bepaald door zakelijke behoefte) voor apparatuur nodig voor kritische bedrijfsprocessen;
- Beveiliging tegen onderbreking van nutsvoorzieningen;
- Afscherming van voedings- en telecom kabels.

Behandelen van apparatuur

Bij het onderhouden, verplaatsen of transporteren van apparatuur moet rekening worden gehouden met volgende vereisten:

- Onderhoud, verplaatsing of transport (buiten de organisatie) mag enkel bevoegd en getraind personeel en/of externe medewerkers;
- Apparatuur moet worden onderhouden volgens de onderhoudsvoorschriften van de leverancier;
- Onderhoud of wijziging aan kritieke apparatuur wordt geregistreerd;
- Indien apparatuur uit dienst wordt genomen of voor herstel buiten de organisatie gebracht, moeten gevoelige gegevens verwijderd worden zodat ze niet meer kunnen gereconstrueerd worden (vernietiging of adequaat wissen van gegevens);

Omgaan met documenten

Niet-publieke documenten moeten ook fysiek beschermd worden tegen onbevoegd gebruik. Dit betekent:

- Kritische documenten moeten na gebruik opgeborgen worden in een afsluitbare kast;
- Kritische documenten moeten opgeborgen worden in een brandvrije kast;
- Toepassen van het *clean desk* en *clear screen* principe;
- Blanco formulieren en toegangsbadges moeten opgeborgen worden in een afsluitbare kast.

2.1.2 Mappen van de zones op informatieklassen

Volgens document ‘kantoor 2023’ wordt een site onderverdeeld in een aantal zones waarvoor er telkens andere beveiligingsvereisten van toepassing zijn. Het document definieert drie beveiligingszones:

- Buitenomgeving: valt buiten scope van het model voor informatieclassificatie.
- Publieke zone: is tijdens kantooruren vrij toegankelijk voor bezoekers.
- Semipublieke zone: is tijdens kantooruren na aanmelding toegankelijk voor bezoekers
- Niet publieke zone: is enkel toegankelijk voor personeel en bezoekers na inschrijving en verificatie.

Klasse 1

- Publieke zones binnen een gebouw zijn locaties waar geen identificatie, authenticatie of autorisatie noodzakelijk zijn.
- Uitgesloten: vergaderzalen in publieke zones (niet auditoria).
- Vb. de inkomhal gebouw Herman Teirlinck (de site Tour&Taxis).

Klasse 2

- Semipublieke zones binnen een gebouw waar een zwakke identificatie noodzakelijk is. Vergaderzalen binnen een ‘publieke zone’.
- Uitgesloten: alle locaties binnen de private zone van een gebouw in gebruik door een organisatie van de Vo.
- Vb. de parking van het gebouw Herman Teirlinck (site Tour&Taxis).

Klasse 3

- Private zone binnen een gebouw, sterke identificatie is noodzakelijk (onthaal of Vo medewerker).
- Binnen deze zone verwerkt men informatie die behoort tot informatieklasse 3.

- Deze behoren tot de niet-publieke beveiligingszone.
- Vb. landschapskantoren.

Klasse 4

- Afgeschermde private zone binnen een gebouw, sterke identificatie en permanente begeleiding is noodzakelijk (onthaal of Vo medewerker).
- Binnen deze zone verwerkt men informatie die behoort tot informatieklasse 4.
- Deze behoren tot de niet-publieke beveiligingszone.
- Vb. specifieke ruimtes van de landschapskantoren.

Klasse 5

- Sterk afgeschermde private zone binnen een gebouw, sterke identificatie en permanente begeleiding is noodzakelijk (onthaal of Vo medewerker).
- Binnen deze zone verwerkt men informatie die behoort tot informatieklasse 5.
- Deze behoren tot de niet-publieke beveiligingszone.

2.2 De werkplek als virtuele locatie

Door de verregaande automatisering van kantoor omgevingen, zijn werkplekken een belangrijke schakel in de bedrijfsvorming geworden. Analoog de architectuur van de locatie waar deze werkplek gebruikt wordt, moeten de nodige maatregelen ter beveiliging genomen worden in de architectuur van de werkplek. Hierbij moet rekening gehouden worden met de klasse van de informatie die op de werkplek verwerkt wordt. We beschouwen de werkplek, of het werkstation daarom als een virtuele locatie.

- Op kantoor kan de werkplek profiteren van maatregelen die niet specifiek voor de werkplek getroffen zijn, maar deze wel een extra bescherming geven, zoals toegangsbewaking, centrale

back-up (beveiliging tegen verlies van informatie), brandbeveiliging, beveiliging tegen stroomonderbreking, functiescheiding, enzovoorts.

- In de thuissituatie worden in het algemeen minder of geen van deze maatregelen getroffen, maar worden nog steeds dezelfde klassen van informatie verwerkt. De thuissituatie wordt aanzien als publieke ruimte (vanuit het standpunt van de organisatie).

Architectuur van de werkplek

De architectuur van de werkplek en de genomen maatregelen moeten rekening houden met

- Het dynamisch aspect van de fysieke locatie (kantoor, op en tijdens verplaatsing)
- Het mobiele aspect van de werkplek (*Portables*)

De genomen maatregelen moeten daarom afgestemd zijn op de fysiek moeilijkst te beveiligen locatie:

- **Statische toestellen** zijn toestellen die de beveiligde fysieke locatie (inclusief het beveiligde netwerk) van de organisatie niet verlaten
- **Mobiele toestellen** zijn toestellen die de beveiligde fysieke locatie van de organisatie, of het beveiligde netwerk verlaten. Het aandeel van tijd doorgebracht binnen- of buiten de fysiek beveiligde locatie of het beveiligde netwerk heeft geen invloed op de mobiele toestand van het toestel. De meest gevoelige toestellen zijn deze toestellen die op regelmatige basis mee op verplaatsing worden genomen, of verbinden met een ander netwerk dan het beveiligde netwerk van de organisatie.

Er kan onderscheid gemaakt worden naargelang het type werkstation dat op de werkplek gebruikt wordt:

- Een **kiosk toestel** is niet verbonden met het Vo netwerk. Bijvoorbeeld een computer verbonden met het internet die ter beschikking wordt gesteld aan bezoekers van een opleidingscentrum.
- Een **kantoor toestel** is gekoppeld aan een Vo netwerk en heeft slechts een beperkte verwerkingscapaciteit; de gestructureerde gegevensopslag vindt niet lokaal plaats. Het toestel omvat enkel generieke functionaliteiten. Het toestel is voornamelijk gebruikt voor administratieve toepassingen.
- Een **gespecialiseerd toestel** is gekoppeld aan een Vo netwerk. Een belangrijk deel van de informatieverwerking vindt lokaal plaats. Het toestel omvat zowel generieke als gespecialiseerde functionaliteiten.
- Voorbeeld: werkstation voor toepassing ontwikkelaars

De logische koppeling van toestellen wordt beschreven in het document *Vo Informatieclassificatie - Minimale maatregelen – netwerken*.

Opmerking:	*De vorm waaronder de werkplek voorkomt heeft geen invloed op bovenstaande classificatie. De computer kan een desktopmodel of een mobiele computer (laptop, notebook, tablet, smartphone…) zijn.*

2.2.1 Maatregelen binnen de werkplek

Maatregelen tegen brand.

Hierbij kan gedacht worden aan brandalarm, brandblussers, enzovoorts. Indien gegevensverwerking en -opslag lokaal plaatsvindt, dan is meer heil te verwachten van back-up van lokale media.

Maatregelen tegen onbeschikbaarheid van de werkplek.

Ook hiervoor geldt dat back-up belangrijk is voor werkplekken waar gegevensverwerking en -opslag lokaal plaatsvindt. Omdat er veelal meerdere uitwisselbare werkplekken zijn, is redundantie in apparatuur vaak automatisch geregeld voor werkplekken.

Maatregelen tegen stroomstoring

Omdat werkplek computers meestal ongevoelig zijn voor het wegvallen van de spanning, hoeven er waarschijnlijk geen maatregelen getroffen te worden. Als dat wel het geval is, of als de continuïteit van de werkplek van essentieel belang is, dan kan een noodstroomvoorziening (UPS) ingezet worden.

Maatregelen tegen diefstal

Vaste werkplekken kunnen relatief eenvoudig tegen diefstal van apparatuur beveiligd worden met behulp van kabels, sloten, bewakers, en dergelijke. Dit geldt in mindere mate voor diefstal van kleine apparatuur: mobiele apparatuur, zoals een notebook of smartphone. Het loont de moeite om hiervoor maatregelen te treffen die de schade bij diefstal beperken. Een belangrijke regel hierbij is dat medewerkers niet met meer apparatuur op stap gaan dan ze nodig hebben. Bovendien kan cryptografie ingezet worden om vertrouwelijke informatie tegen niet geautoriseerde toegang te beschermen (voor meer informatie zie document: '*Vo Informatieclassificatie - Minimale maatregelen – Cryptografie*').

2.2.2 Mappen van de werkplek op informatieklassen

Wat betreft locatie, onderscheiden we volgende types, gemapt op de informatieklassen:

Klasse 1

- Werkplekken in publieke zones: deze zijn toegankelijk voor iedereen, bijvoorbeeld een desktop in een opleidingscentrum of onthaalzone toegankelijk voor gebruikers om het internet te raadplegen.
- Uitgesloten: vergaderzalen in publieke zones (niet auditoria).

Klasse 2

- Werkplekken in publieke zones waar een zwakke identificatie noodzakelijk is. Vergaderzalen binnen een 'publieke zone'.
- De werkplek thuis kan beschouwd worden als klasse 2 omdat de mogelijkheden tot beveiliging en controle beperkt zijn.
- Uitgesloten: alle locaties binnen de private zone van een gebouw in gebruik door een organisatie van de Vo.

Klasse 3

- Werkplekken in een private zone, waar slechts beperkte toegang toegelaten is.
- Op deze werkplek verwerkt men informatie die behoort tot maximaal informatieklasse 3.

Klasse 4

- Werkplek in een afgeschermde private zone waar slechts beperkte toegang toegelaten is.
- Op deze werkplek kan informatie die behoort tot informatieklasse 4 verwerkt worden.

Klasse 5

- Werkplek in een sterk afgeschermde private zone met zeer beperkte toegankelijkheid.
- Op deze werkplek kan informatie die behoort tot informatieklasse 5 verwerkt worden.

3 LINK MET ANDERE MAATREGELEN

3.1 Link met IAM als maatregel

Fysieke toegangsbeveiliging is complementair aan logische toegangsbeveiliging, wat verder uitgelegd wordt in het document: *'Vo Informatieclassificatie - Minimale maatregelen – IAM'*.

3.2 Link met logging als maatregel

Fysieke beveiliging gaat vaak gepaard met logging, enkele voorbeelden zijn:

- Het bijhouden van bezoekersregistratie of een bezoekerslogboek;
- Het bijhouden van een onderhoudslogboek;

Manuele logboeken zijn echter onderhevig aan fouten en vragen de nodige discipline en de capaciteit van de uitvoerders om deze taak systematisch en precies te herhalen. Bovendien zijn er vaak meerdere uitvoerders bij betrokken, wat het risico op fouten vergroot.

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.

3.3 Link met functiescheiding

Het scheiden van functies als basismaatregel voor informatiebeveiliging volgt in lijn de arbeidsverdeling van de organisatie. In hoofdlijnen worden processen gescheiden uitgevoerd.

Globaal gelden de volgende functiescheidingen:

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

Elke dienst heeft een eigen taak binnen de organisatie en voert deze zelfstandig uit.

Fysieke toegangsbeveiliging is erop gericht om gebouwen en informatie te beschermen door ongeautoriseerde toegang te voorkomen en kent haar eigen functiescheiding:

- Eigen medewerkers versus bezoekers: eigen medewerkers worden niet als bezoeker aangemerkt. Alleen aan personen de geen deel uitmaken van de organisatie worden bezoekerspassen verstrekt.
- Extern onderhoudspersoneel: deze maken geen deel uit van de eigen organisatie en dienen in principe 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).