Zuyd Security Beleid – Baseline Informatiebeveiliging

Versie 1.2

Vastgesteld door het CvB op 21-10-2025

Inhoudsopgave

1. Documentenbeheer

Revisiehistorie

Revisiedatum	Samenvatting veranderingen	Door	Versie
15-10-2023	Draft versie	D. Heynen	0.1
12-02-2024	Verder uitwerking/verdieping	D. Heynen	0.4
12-03-2024	Review CISO/ISO	D. Heynen	0.6
02-04-2024	Concept versie voor CvB incl. opmerkingen stakeholders.	D. Heynen	0.8
02-07-2024	Zuyd Security Beleid – Baseline Informatiebeveiliging vastgesteld door CvB.	R. Sterken	1.0
09-09-2025	Minor Update, template Zuyd, url koppelingen, tekstuele aanpassing.	D. Heynen	1.1
21-10-2025	Vastgesteld door CvB	R. Sterken	1.2

Documentatie
Er is gebruik gemaakt van de onderstaande informatie

Naam	Auteur	Status
Informatiebeveiligingsbeleid Zuyd Hogeschool versie 2025	CISO Zuyd Hogeschool	Definitief
Normenkader Informatiebeveiliging versie 2.0	SURF	Definitief
Security Baseline voor onderwijs en onderzoek	SURF	Definitief
Security Baseline Controls SURF	SURF	Definitief
Baseline Informatiebeveiliging Rijksdienst Tactisch normenkader	Min. Van Binnenlandse Zaken en Koninkrijksrelaties	Definitief
Enterprise Architectuur – Application Rules	CIO Zuyd Hogeschool	Definitief
Privacy & Security Risicomanagement	CISO Zuyd Hogeschool	Definitief

Jaarlijkse vaststelling

Dit document is vastgesteld door:

Naam	Uitgiftedatum	Versie
CvB	21 oktober 2025	1.2

2. Managementsamenvatting

Dit beleid omvat de baseline informatiebeveiliging (basismaatregelen) voor Zuyd en is opgesteld om de Zuyd ICT-Infrastructuur te beschermen tegen ongeoorloofde toegang of wijziging, met als doel de **beschikbaarheid, integriteit** en **vertrouwelijkheid** van de informatie te waarborgen.

Als baseline informatiebeveiliging volgt Zuyd de Surf Security baseline (daar waar nodig geacht aangevuld met additionele maatregelen). Buiten de SURF richtlijnen heeft Zuyd aanvullende, vervangende of specifieke richtlijnen in de vorm van Zuyd security beleid. Met de baseline informatiebeveiliging wil Zuyd minimumeisen aan de beveiligingsinstellingen voor de gehele Zuyd ICT-Infrastructuur stellen, ongeacht of deze door FB-ICT of door externe leveranciers wordt geleverd/beheerd.

Deze baseline dient als leidraad om duidelijkheid te scheppen over de beveiliging van de informatievoorziening met betrekking tot **beschikbaarheid, integriteit** en **vertrouwelijkheid**. Ook moet het duidelijkheid scheppen over de verantwoordelijkheden van proces- en systeemeigenaren en hoe deze verantwoordelijkheden ingevuld dienen te worden.

In grote lijn betekent de baseline informatiebeveiliging voor Zuyd het volgende:

1. Voor de gehele Zuyd ICT-Infrastructuur worden als uitgangspunt de richtlijnen (basismaatregelen) van de SURF Security baseline gehanteerd. Daarnaast is er het Zuyd Security beleid (zie Bijlage 1) met aanvullende, vervangende of specifieke security richtlijnen.
2. Zuyd hanteert het pas toe of leg uit principe en legt de verantwoordelijkheid in de 1ste lijn. De proces en/of systeemeigenaar kan dus afwijken van de richtlijnen, maar moet dit goed onderbouwen en vastleggen conform privacy & risicomanagement proces. Afwijkingen gaan in overleg met de betreffende adviseur (CISO en/of ISO).
3. Afwijkingen van de richtlijnen worden verwerkt middels het door het CvB vastgestelde privacy & security risicomanagement proces.
4. De verantwoordelijkheid voor de implementatie van de richtlijnen ligt bij de systeemeigenaar en/of de proceseigenaar.
5. Bepaalde richtlijnen worden organisatiebreed uitgevoerd, niet altijd kan de systeem- en/of proceseigenaar deze namelijk zelfstandig toepassen.
6. De richtlijnen (zie Bijlage 2) zijn afhankelijk van de BIV-classificatie (zie Tabel 1 en Bijlage 1) van het systeem/proces waar vastgesteld door IM.

Classificatie:	Richtlijn Zuyd	Richtlijn SURF hoog	Richtlijn SURF midden	Richtlijn SURF laag
B, I of V hoog	x	x	x	x
B, I of V midden	x		x	x
B, I of V laag	x			x
BIV niet gespecificeerd	x	x	x	x

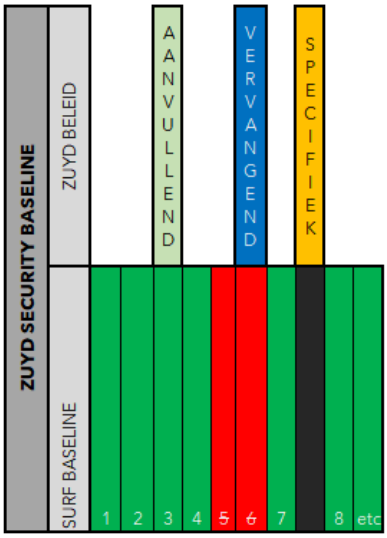
Tabel 1: Richtlijnen in relatie tot BIV classificatie

7. De voor het betreffende systeem ingerichte richtlijnen worden periodiek door de proces en/of systeemeigenaren beoordeeld op naleving en actualiteit van de baseline informatiebeveiliging.

3. Zuyd Security Beleid – Baseline Informatiebeveiliging

3.1. Inleiding

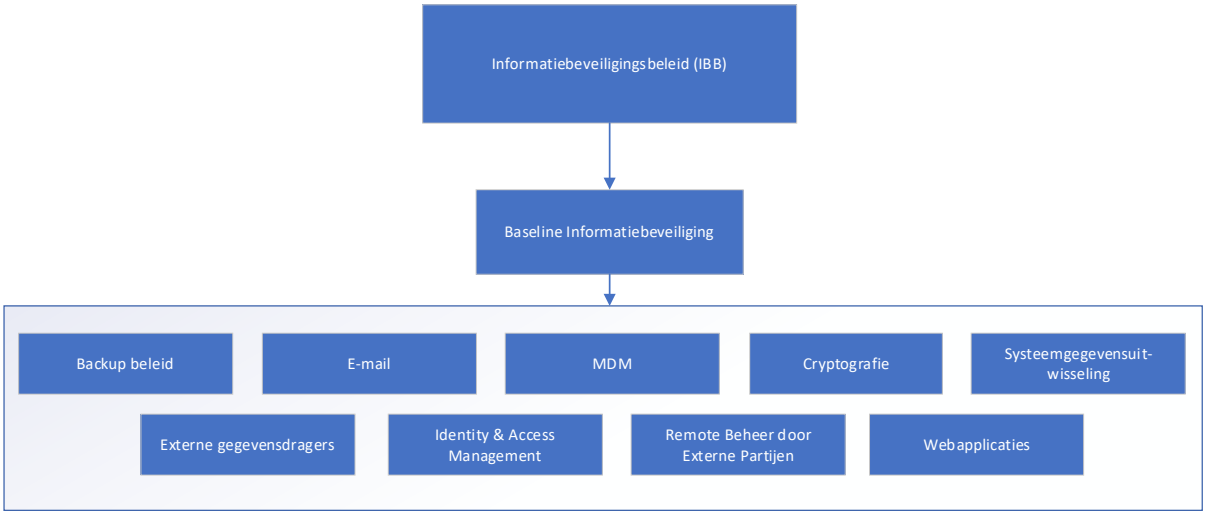
In het informatiebeveiligingsbeleid worden de randvoorwaarden en uitgangspunten vastgelegd en wordt richting gegeven aan de vertaling van beleid in concrete maatregelen. De baseline informatiebeveiliging van Zuyd is een verdere uitwerking die concrete maatregelen in de vorm van richtlijnen bevat. Deze zijn van toepassing op de Zuyd ICT-Infrastructuur met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid. De baseline informatiebeveiliging schept duidelijkheid over de verantwoordelijkheden van proces- en systeemeigenaren en hoe deze verantwoordelijkheden ingevuld dienen te worden. Bepaalde richtlijnen worden organisatiebreed uitgevoerd, daar de systeem- of proceseigenaar deze niet altijd zelfstandig kan inregelen.



Figuur 1: Opbouw Richtlijnen Zuyd Security Baseline

Zuyd volgt de Surf Security baseline om een minimumvereiste aan de beveiligingsinstellingen te stellen voor de gehele Zuyd ICT-Infrastructuur[1] met als uitgangspunt de BIV classificatie van het systeem/proces, ongeacht of FB-ICT of een externe leverancier daar verantwoordelijk voor is. De Surf Security baseline wordt door SURF vastgesteld voor het hoger onderwijs. De baseline van SURF is gebaseerd op verschillende normen, zoals de ISO 27001- en STITCH-controls

Zuyd conformeert zich aan deze SURF standaard, met waar nodig geacht additionele richtlijnen (maatregelen), als uitgangspunt voor alle Zuyd IT-producten en diensten. Buiten de SURF richtlijnen heeft Zuyd aanvullende, vervangende of specifieke richtlijnen in de vorm van Zuyd securitybeleid (zie Fig.1 & 2).



Figuur 2: Overzicht Zuyd security beleid (Baseline, Backup, E-mail, MDM etc)

[1] Zuyd IT-Infrastructuur: het geheel van ICT-voorzieningen om Zuyd te ondersteunen bij processen zoals financiën, onderwijs, onderzoek, planning, rapportages en communicatie. Door het verwerken, opslaan, en transporteren van digitale data.

3.2. Relatie tot SURF CMM Toetsingskader

Dit beleid is gekoppeld aan de uitgangspunten in het SURF Audit Toetsingskader[1]. SURF schrijft: "De meest geaccepteerde internationale standaard op het gebied van informatiebeveiliging is ISO27002:2013. Wij hebben ons normenkader hierop gebaseerd". Uit deze ISO-norm zijn de onderdelen geselecteerd die een onderwijsinstelling in ieder geval geregeld moet hebben.

Het beleid heeft sterke raakvlakken met meerdere beheers doelstellingen uit dit kader (te weten: NBA ID: CO.01, CO.02, CH.04, DM.03, DM.05, DM.06, ID.01, ID.02, SM.01, SM.02, SM.03, SM.04, SM.05, SM.06, SM.07, SM.08, SM.09, SM.10, SM.11, SM.12, SM.13, OP.01, OP.03, OR.01 en PH.01) maar dient met name als een uitwerking van de beheersdoelstelling **NBA ID: SM.01** in het domein ***Security Management***.

3.3. Relatie tot overige documenten

Naast dit beleidsdocument zijn de volgende stukken relevant:

- Informatiebeveiligingsbeleid Zuyd (IBB)
  - Het document dat het informatiebeveiligingsbeleid van Zuyd beschrijft.
- Security baseline voor onderwijs en onderzoek SURF v2.0
  - Het document van SURF met de security baseline.
- Enterprise Architectuur - Application Rules
  - Het document met de architectuur- applicatie landschapsrichtlijnen van Zuyd.
- Privacybeleid Zuyd Hogeschool
  - Het document dat het privacybeleid van Zuyd beschrijft.

3.4. Doel

Dit beleid omvat de baseline informatiebeveiliging (basisrichtlijnen) voor Zuyd en is opgesteld om de Zuyd ICT-Infrastructuur te beschermen tegen ongeoorloofde toegang of wijziging, met als doel de **beschikbaarheid, integriteit** en **vertrouwelijkheid** van de informatie te waarborgen.

3.5. Scope

De beleidsuitgangspunten in de baseline informatiebeveiliging hebben betrekking op de Zuyd ICT-Infrastructuur.

3.6. Beleid

Bij invoering of aanpassing van componenten in de Zuyd ICT-Infrastructuur gelden de volgende security richtlijnen:

1. Als uitgangspunt worden de richtlijnen [2] (basismaatregelen) van de SURF Security baseline gehanteerd. Daarnaast is er het Zuyd Security beleid (zie Figuur 2) met aanvullende, vervangende of specifieke security richtlijnen (zie Bijlage 2 – Richtlijnen SURF en Zuyd per categorie).
2. Zuyd hanteert het pas toe of leg uit principe en legt de verantwoordelijkheid in de 1ste lijn. De proces en/of systeemeigenaar kan dus afwijken van de richtlijnen, maar moet dit goed onderbouwen en vastleggen.
3. Afwijkingen van de richtlijnen worden middels het privacy & security risicomanagement proces gedocumenteerd en goedgekeurd (of gecorrigeerd);
4. De verantwoordelijkheid voor de implementatie van de richtlijnen ligt bij de systeemeigenaar en/of proceseigenaar;

[2] De eindverantwoordelijke draagt zorg voor de verplichte implementatie van de organisatie brede controls van de SURF Security Baseline. De proceseigenaar is verantwoordelijk voor een specifiek bedrijfsproces en de daarbij behorende controls. De systeemeigenaar is verantwoordelijk voor het beheer van een bepaald IT-systeem en de daarbij behorende controls. In sommige gevallen kunnen de rollen van proceseigenaar en systeemeigenaar elkaar overlappen of gecombineerd zijn.

5. Bepaalde richtlijnen worden organisatiebreed uitgevoerd, meestal kan de systeem- en/of proceseigenaar deze namelijk niet zelfstandig nemen;
6. De richtlijnen (zie Tabel 2 en Bijlage 1) zijn afhankelijk van de BIV-classificatie van het systeem/proces die is vastgesteld door IM.

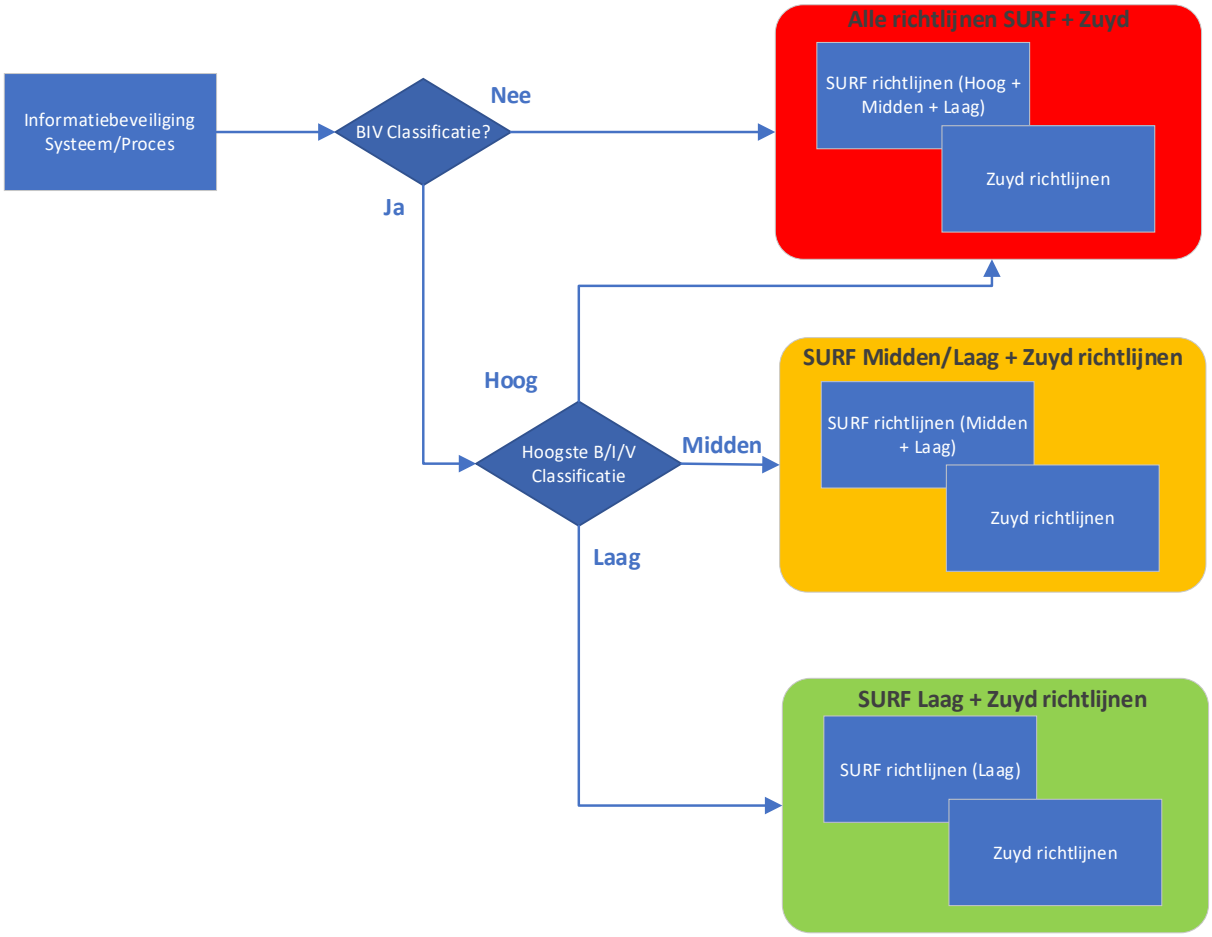
Classificatie:	Richtlijn Zuyd	Richtlijn SURF hoog	Richtlijn SURF midden	Richtlijn SURF laag
B, I of V hoog	x	x	x	x
B, I of V midden	x		x	x
B, I of V laag	x			x
BIV niet gespecificeerd	x	x	x	x

Tabel 2: Richtlijnen in relatie tot BIV classificatie

7. Het is de verantwoordelijkheid van de proces of systeemeigenaar om periodiek te controleren dat deze richtlijnen gevolgd worden.
    a. Resultaten worden gedocumenteerd;
    b. Afwijkingen van de richtlijnen meldt de eigenaar aan de ISO die deze middels het door het CvB vastgestelde privacy & security risicomanagement proces documenteert

De CISO en ISO's van Zuyd houden toezicht op het volgen van dit beleid. Afwijkingen dienen via de CISO/ISO aangevraagd te worden.

Bijlage 1 – Richtlijnen in relatie tot BIV Classificatie

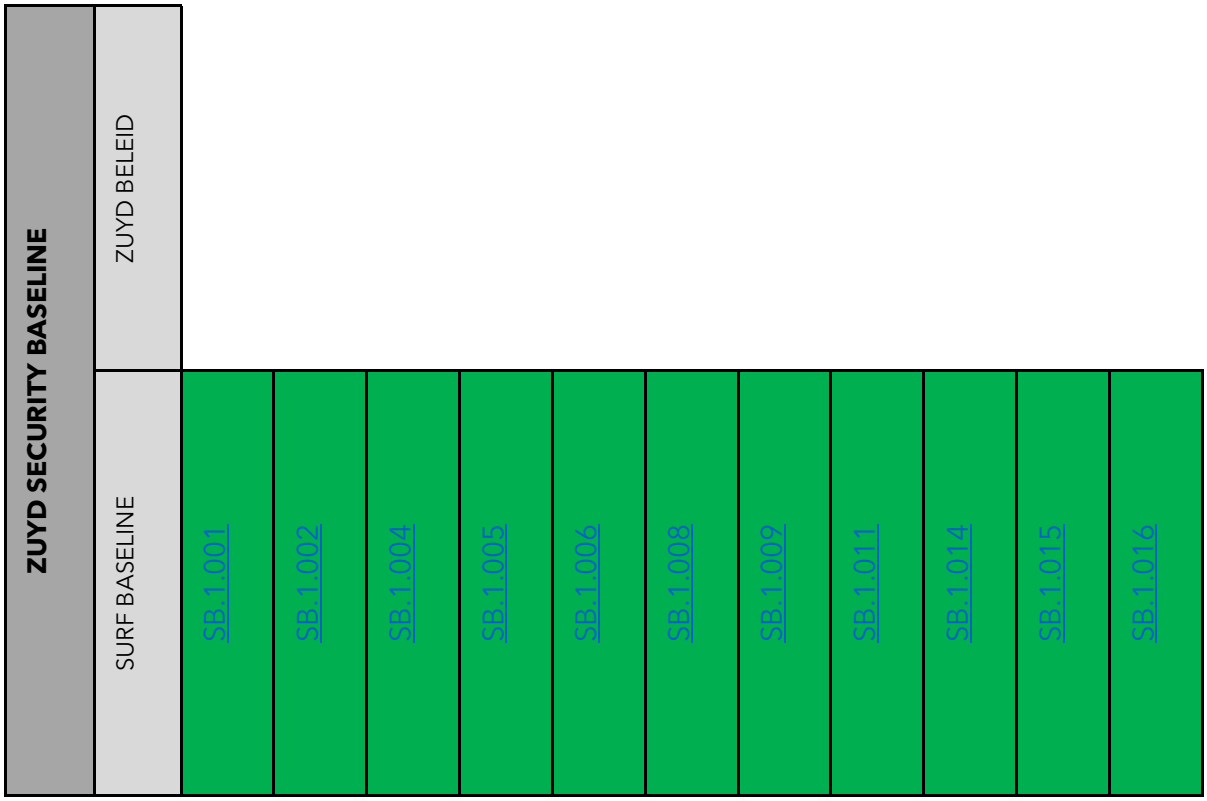


Figuur 3: Richtlijnen in relatie tot BIV classificatie Zuyd systeem/proces

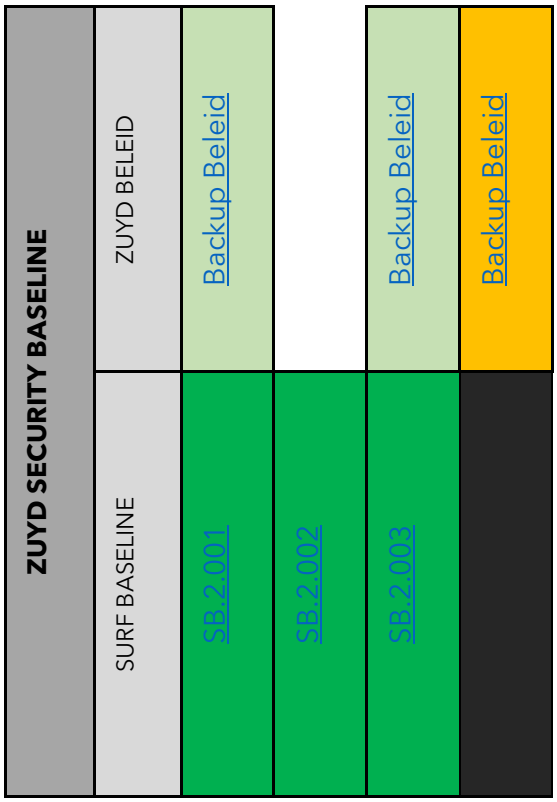
Bijlage 2 – Richtlijnen Surf & Zuyd per categorie

Legenda:

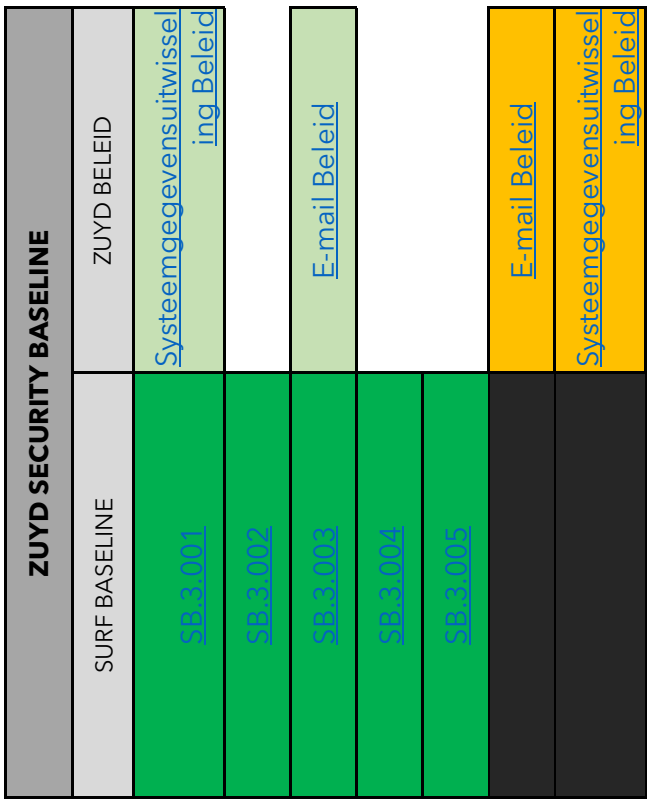
- *Surf richtlijn toepassen*
- *Surf richtlijn vervalt*
- *Surf richtlijn ontbreekt*
- *Zuyd aanvullende richtlijn*
- *Zuyd vervangende richtlijn*
- *Zuyd specifieke richtlijn*



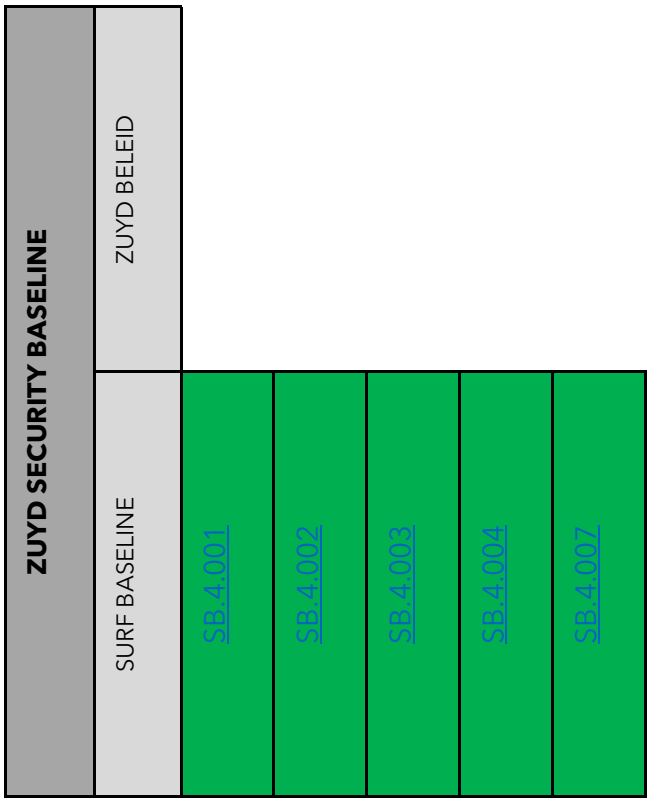
Figuur 4: Richtlijnen in de categorie Asset Management



Figuur 5: Richtlijnen in de categorie Backup & Restore

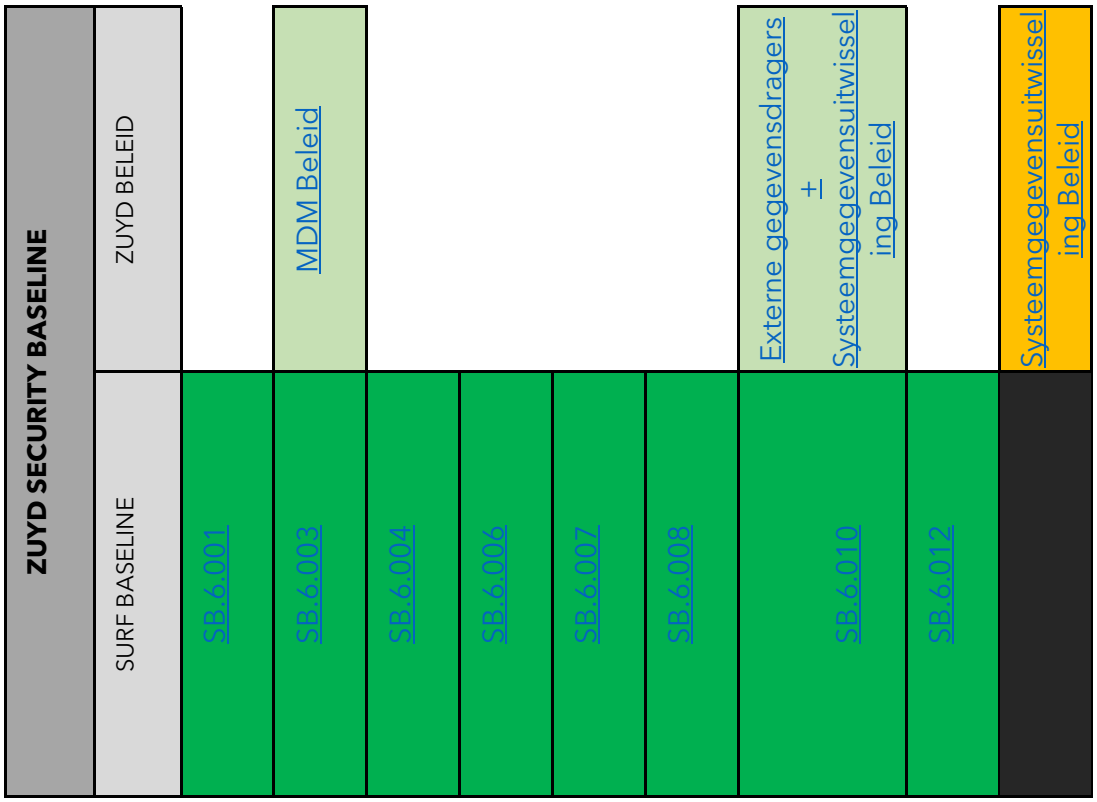


Figuur 6: Richtlijnen in de categorie Communications Security

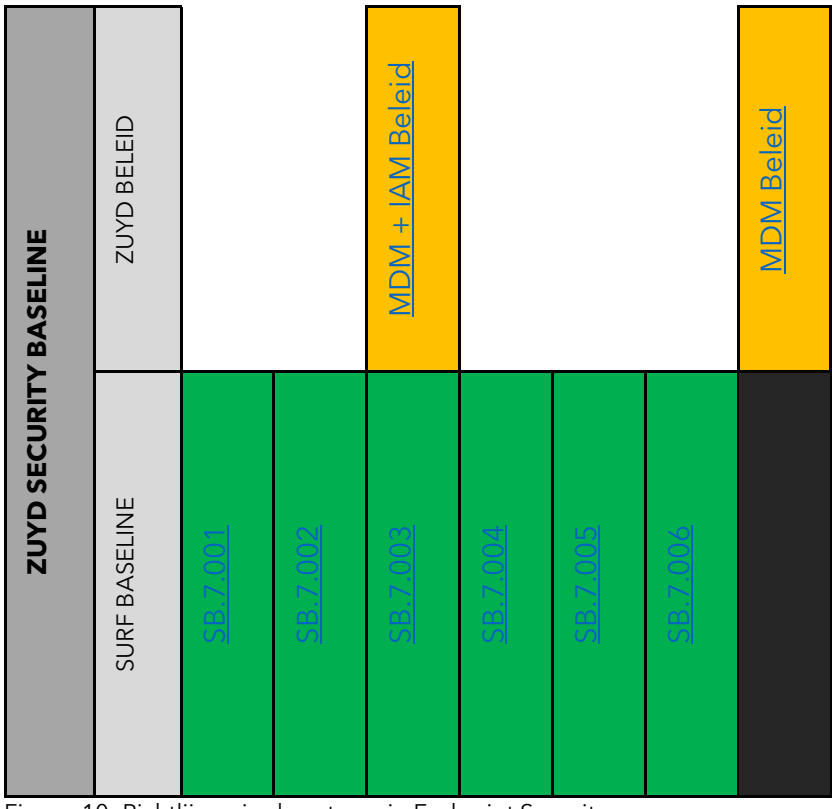


Figuur 7: Richtlijnen in de categorie Crisis & Incident Response

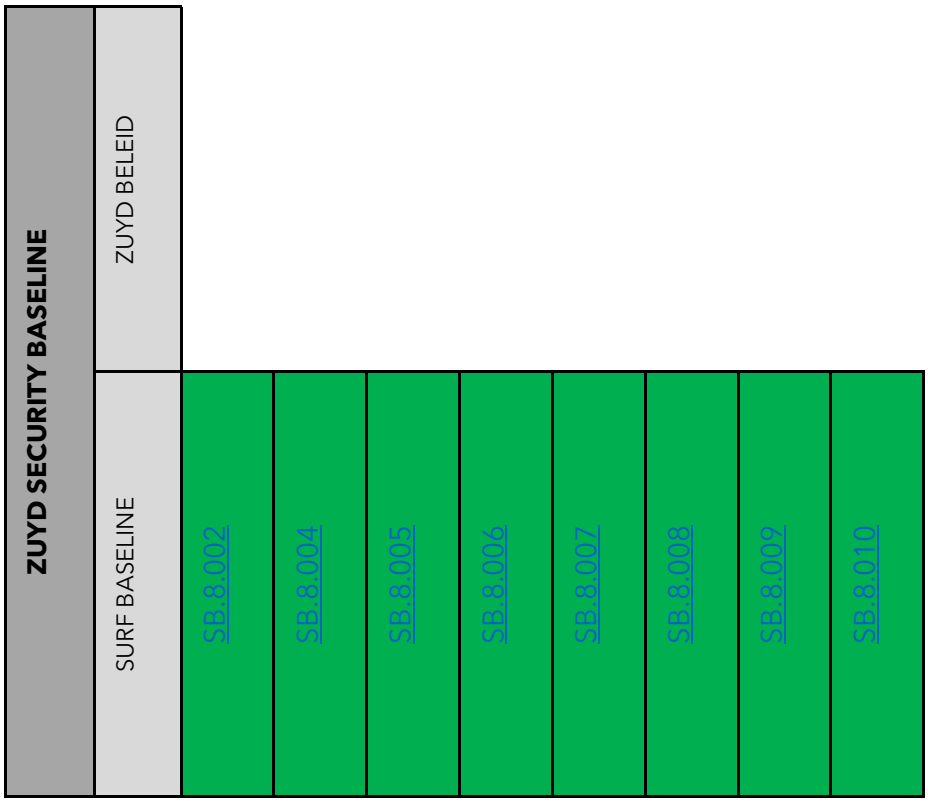
Figuur 8: Richtlijnen in de categorie Cryptography



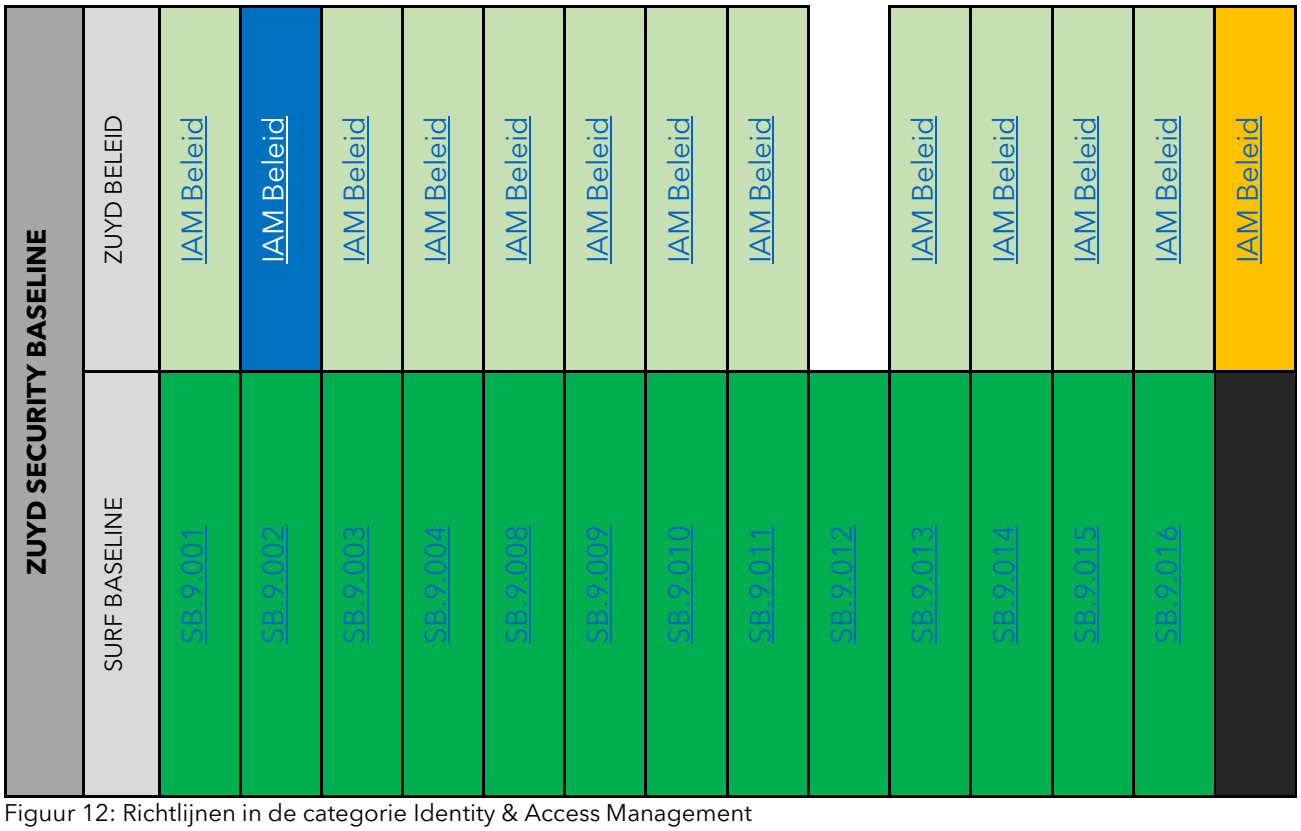
Figuur 9: Richtlijnen in de categorie Data Protection



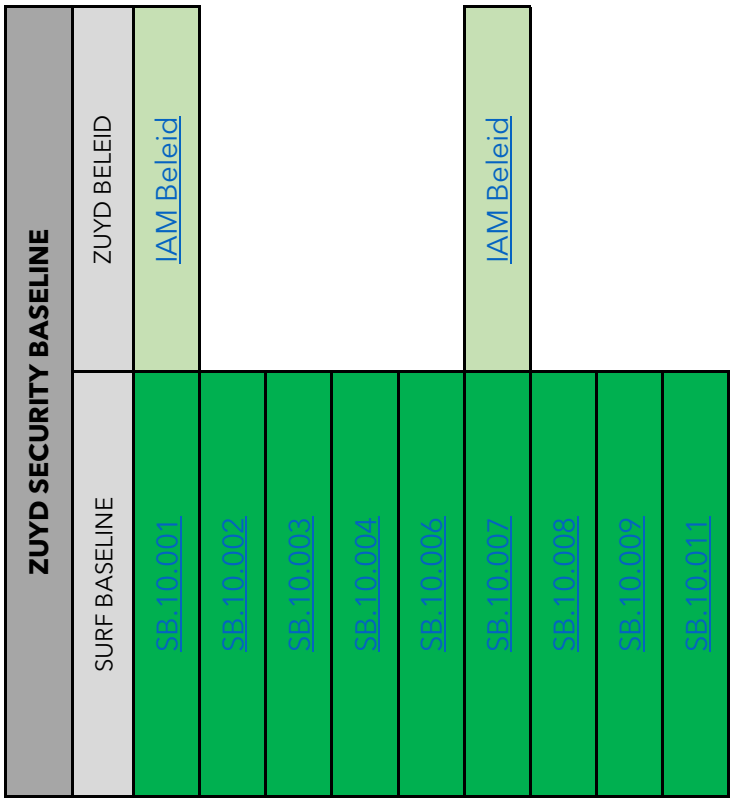
Figuur 10: Richtlijnen in de categorie Endpoint Security



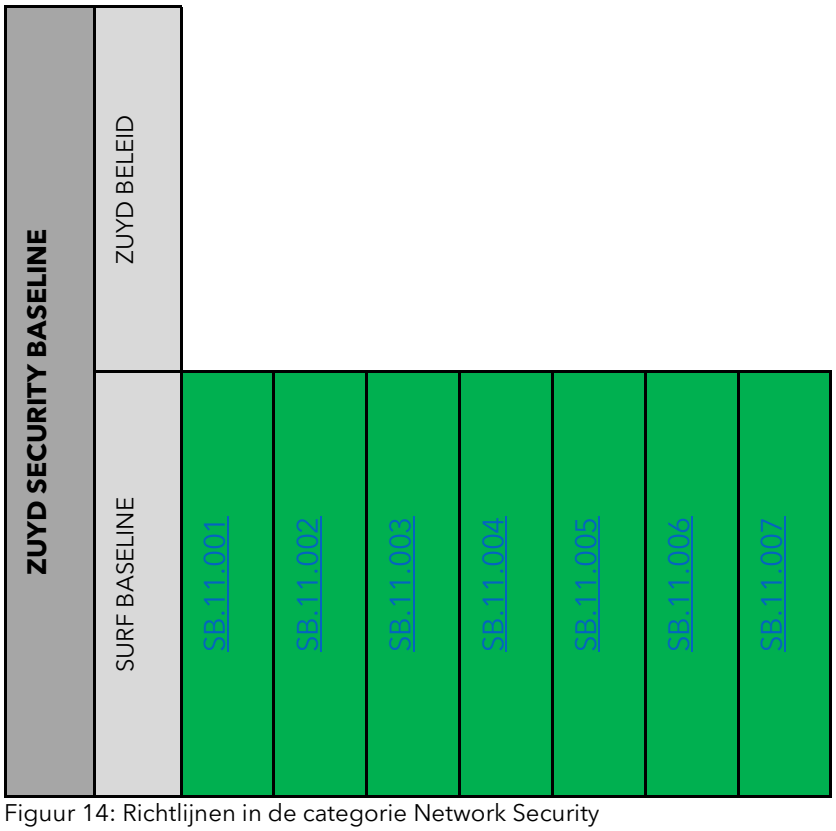
Figuur 11: Richtlijnen in de categorie Human Resource Security



Figuur 12: Richtlijnen in de categorie Identity & Access Management

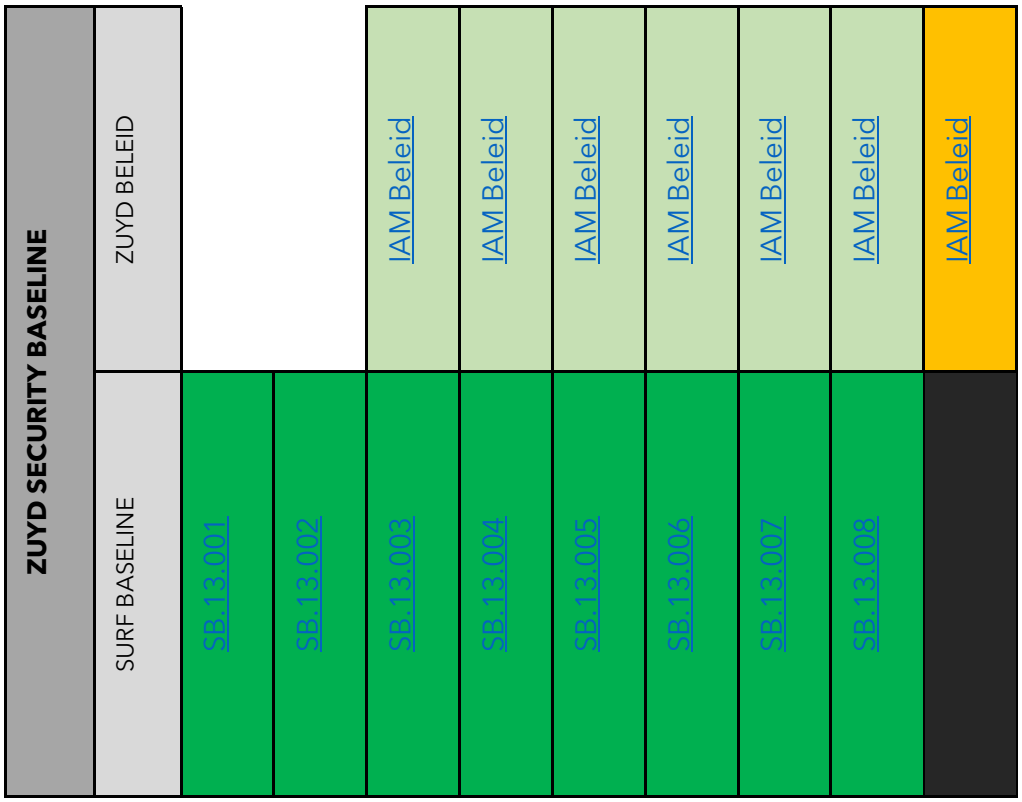


Figuur 13: Richtlijnen in de categorie Logging & Monitoring

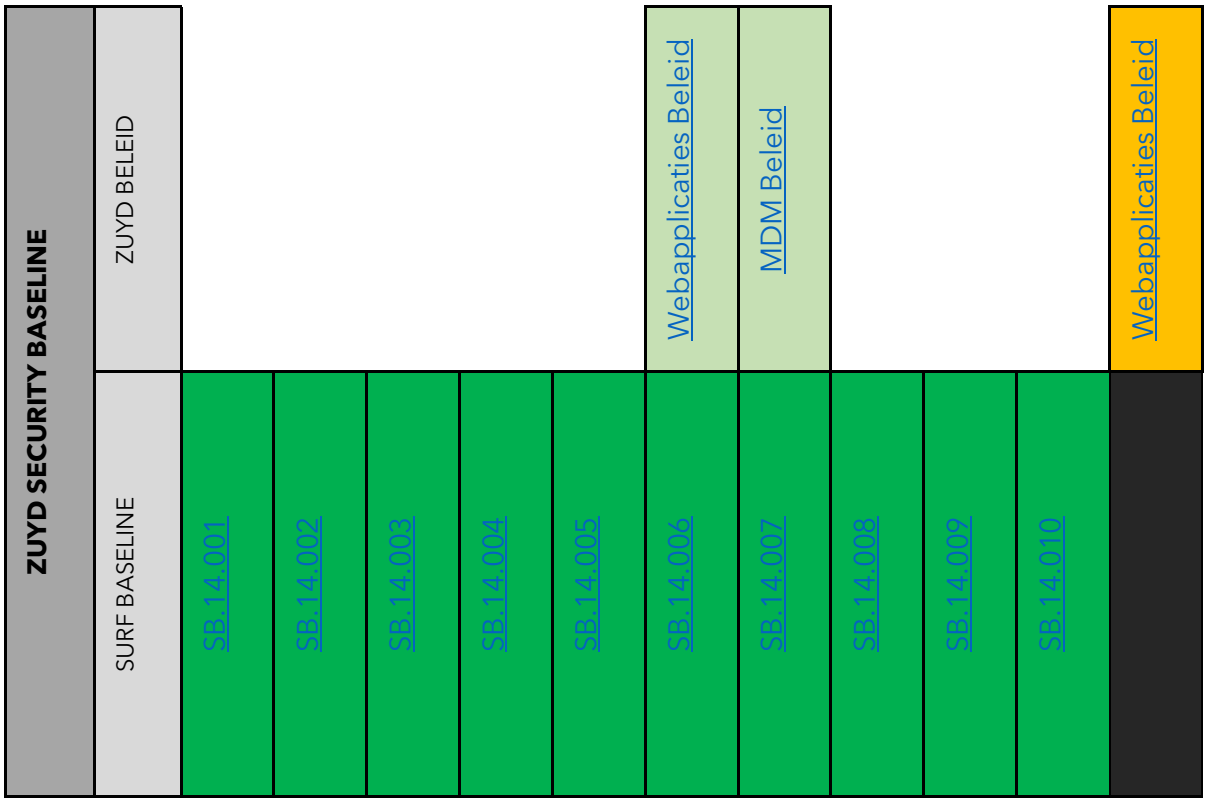


Figuur 14: Richtlijnen in de categorie Network Security

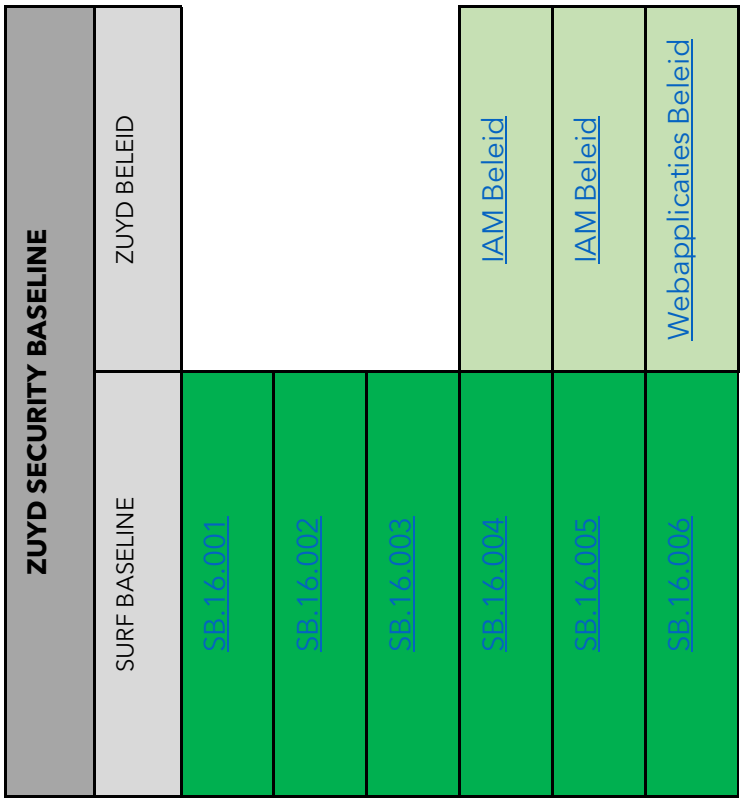
Figuur 15: Richtlijnen in de categorie Physical & Environmental Security



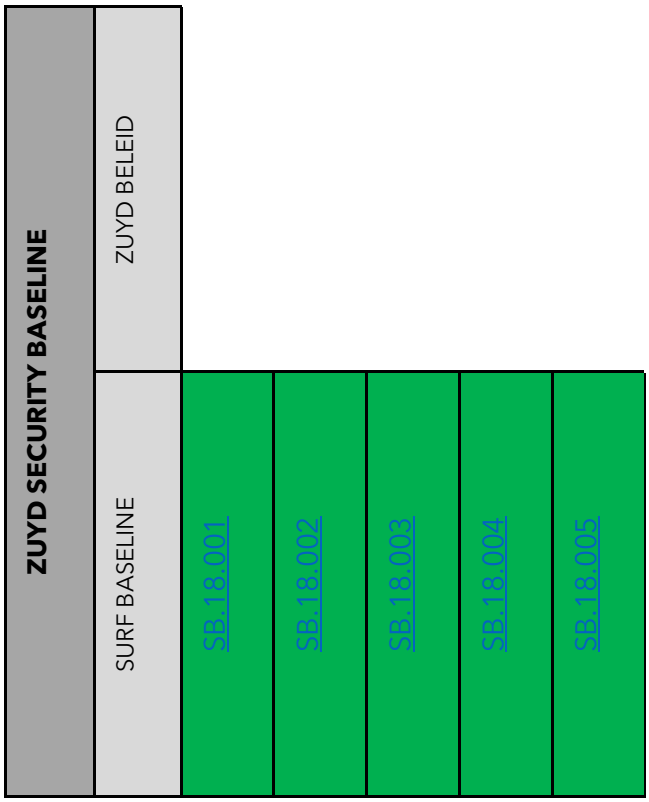
Figuur 16: Richtlijnen in de categorie Priviliged Access Management



Figuur 17: Richtlijnen in de categorie Secure Development



Figuur 18: Richtlijnen in de categorie System Hardening



Figuur 19: Richtlijnen in de categorie Vulnerability Management