



Rijksvastgoedbedrijf
Ministerie van Binnenlandse Zaken en
Koninkrijksrelaties

Cybersecurity Raamwerk Vastgoed Gebonden Systemen

*Een **standaard** / **basis** voor de Vastgoed Gebonden Systemen zodat deze weerbaar en robuust zijn om de comfort en veiligheid van gebouwen te waarborgen.*



INTERN VERTROUWELIJK



Colofon

Versie: 1.9

Status: definitief

Datum: 27-7-2026

Contact:

Rijksvastgoedbedrijf (RVB)

postbus.rvb.cybersecurityVGS@rijksoverheid.nl

www.rijksvastgoedbedrijf.nl

Auteur(s):

Rijksvastgoedbedrijf | T&P | A&T | Digitalisering & Beveiliging

Rijksvastgoedbedrijf | VB | TE | Technisch Advies Installatietechniek



Document geschiedenis

Revisies

Versie	Status	Datum	Aanpassingen
1.2.6	Definitief	25-01-2024	Goedgekeurd in Beleidsoverleg Rijksvastgoedbedrijf. Dient niet meer in nieuwe projecten na 27 juli 2026 toegepast te worden en wordt vervangen door deze versie.
1.9	Definitief	27-7-2026	Wijzigingen structuur en integratie beheerorganisatie.



Inhoudsopgave

COLOFON 2

DOCUMENT GESCHIEDENIS 3

1 INLEIDING & ALGEMEEN 7

1.1	Doel	7
1.2	Structuur van dit document	7
1.3	Scope - Vastgoed Gebonden Systemen	7
1.4	Informatiebeveiliging versus Cybersecurity	8
1.5	Cybersecurity VGS in verschillende fasen	9
1.6	Wat wordt van u verwacht?	9
1.7	Algemene uitgangspunten	10
1.8	Wet- en regelgeving, normenkaders en benchmarks	12

2 RISICOMANAGEMENT & CLASSIFICATIE VGS EN DATA 14

2.1	Classificatie/Rubricering	14
2.2	Risicomanagement / Business impact analyse VGS	15
2.3	Risicodossier / Compliance	16
2.4	Verwerking van persoonsgegevens	17
2.5	Beschermen registraties en Bewaartermijnen	17
2.6	Eigendom gegevens	18

3 PRINCIPES & ARCHITECTUUR 19

3.1	Visie en beleid	19
3.2	Principes	19
3.3	Scope en blauwdruk van de netwerk- & systeemarchitectuur	20
3.4	VGS CS Referentiearchitectuur (CSRA)	21
3.5	Blauwdruk – high- & low-level design	24
3.6	Landen met een actief offensief cyberprogramma tegen Nederland	24

4 NETWERKARCHITECTUUR & VERBINDINGEN 25

4.1	Begripsvorming	25
4.2	Professioneel netwerkontwerp en beheer	26
4.3	Netwerk Resilience	28
4.4	Netwerksegmentatie	29
4.5	Externe connectiviteit – Toepassing	30
4.6	Externe Connectiviteit – Vereisten	32
4.7	Inrichting Update proces	34
4.8	Draadloze technologie – registratie en goedkeuring	35
4.9	Netwerktogang & authenticatie	36
4.10	Versleuteling communicatie – data in transit	37
4.11	Veilige protocollen	38

5 VASTGOED GEBONDEN SYSTEMEN 39

5.1	Betrouwbaar & Robuust	39
5.2	Hardening	39
5.3	VGS Resilience	40
5.4	Versleuteling – data at rest	41



5.5	Mobiele apparatuur	42
5.6	Specifiek	42
6	KOPPELVLAKKEN TUSSEN SYSTEMEN	44
7	SECURITY MONITORING & DETECTIE	46
7.1	Tijdsynchronisatie	46
7.2	Logging & analyse	46
7.3	Security Monitoring	47
7.4	Health Monitoring	49
7.5	Bewaking bewaartermijnen logging	50
7.6	Detectie & preventiemechanismen	51
8	STAATSGEHEIM	52
8.1	VGS in staatsgeheime ruimte	52
8.2	VGS in een staatsgeheim gebouw	54
8.3	VGS met rubricering STAATSGEHEIM	54
9	CLOUDDIENSTEN	56
9.1	Cloud-architectuur	56
9.2	Dataontsluiting	57
9.3	Netwerkbeveiliging	57
9.4	Logische toegang	57
9.5	Bescherming van data	58
9.6	Security monitoring	58
9.7	Security assurance	58
10	FYSIEKE BEVEILIGING	60
10.1	Fysieke toegang & begeleiding	60
10.2	Ruimtes	60
10.3	Systemen	60
10.4	Bekabeling	60
11	SECURITY CONFIGURATIE & PROCESSEN	61
11.1	Lifecycle management	61
11.2	Asset- & configuratiemanagement	61
11.3	Wijzigingsbeheer	62
11.4	Kwetsbaarheden- en Patchmanagement	62
11.5	Logisch toegangsbeheer	63
11.6	Back-up en herstel	65
11.7	Incident- & response management	66
11.8	Bedrijfscontinuïteit en disaster recovery plannen	67
12	ORGANISATIE & GOVERNANCE	68
12.1	Overlegstructuur en Rapportage	68
12.2	Proces- & documentmanagement	68
12.3	Rollen en verantwoordelijkheden	68
12.4	Personeelsmanagement	69
12.5	Bewustwording en training	69
12.6	Transport van gegevens	70
12.7	Vernietiging van gegevens	70
12.8	Contract- & leveranciersmanagement	70



13	ASSURANCE, TOETSING & RAPPORTAGE	71
13.1	Certificeringen/audits organisatie, systemen & producten	71
13.2	Testmomenten	71
13.3	Security Assurance	73
13.4	Penetratietesten (pen-testen)	73
14	OVERDRACHT NAAR BEHEER	75
14.1	Overdracht naar nieuwe beheerorganisatie	75
BIJLAGE A : AFKORTINGEN & BEGRIPPEN.....		77
BIJLAGE B : RUBRICERINGSMATRIX		82
BIJLAGE C : VERWIJZINGEN		83
Verwijzing 01:	Sjabloon Cybersecurityplan (CSP)	83
Verwijzing 02:	VGS Business Impact overzicht	83
Verwijzing 03:	Instructie inventarisatie VGS.....	83
Verwijzing 04:	Instructie classificatie VGS	83
Verwijzing 05:	Instructie PEN-testen	83
Verwijzing 06:	VGS CS Architectuur documenten.....	83
BIJLAGE D : VOORBEELD ONTWERP TOEPASSING SCRUBBER.....		84
BIJLAGE E : SPECIFICATIE RAPPORTAGE VGS		86
BIJLAGE F : DO'S EN DON'TS ACCEPTABEL GEBRUIK		87
BIJLAGE G : CMDB.....		88



1 INLEIDING & ALGEMEEN

1.1 Doel

Dit Cybersecurity Raamwerk Vastgoed Gebonden Systemen is bedoeld voor Opdrachtnemers van het Rijksvastgoedbedrijf. In dit Cybersecurity Raamwerk (CSR) zijn de cybersecurityeisen verwoord ten aanzien van Vastgoed Gebonden Systemen (VGS). Het Rijksvastgoedbedrijf heeft als doel te allen tijde te borgen dat alle VGS voldoende weerbaar en robuust zijn, zodat de functionaliteit, het comfort en de veiligheid van onze gebouwen behouden blijven. Om dit te realiseren dienen beheersmaatregelen te zijn genomen om de cybersecurity van de VGS professioneel invulling te geven. Voorop staat een passende, risico-mitigerende inrichting van VGS, zodat (niet limitatief):

- De bedrijfscontinuïteit van VGS afdoende is geborgd.
- De kwaliteit van de dienstverlening is geborgd.
- De veiligheid van mensen is geborgd.
- Kritische bedrijfsprocessen niet worden verstoord.
- Het gebouw(deel) of complex in haar functie kan blijven voorzien.
- Persoonsgegevens en vertrouwelijke informatie niet in handen komt van onbevoegden.
- De (informatie-)beveiliging van de Gebruiker niet ondermijnd wordt.

Het is van belang dat dit als een bedrijfsbelang is geborgd in de *governance*, zodat het geheel van gebouwinstallaties gedurende de gehele levensduur in voldoende mate beschermd is.

1.2 Structuur van dit document

Dit document is als volgt gestructureerd:

- Blauwe tekst betreft achtergrond en/of toelichting.
- Zwarte, gekaderde tekst met nummering bevatten expliciete eisen
- Oranje zijn vereiste inputdocumenten
- Grijs zijn algemene interne verwijzingen
- [Hyperlinks bevatten externe verwijzingen naar openbare bronnen](#)

De eisen in dit document zijn als volgt gekenmerkt:

A	Algemeen, architectuur, principes (te borgen in ontwerp-, realisatie- en beheerfase).
O	Ontwerpeis (te borgen in realisatie- en beheerfase).
R	Realisatie-eis (te borgen tijdens beheerfase).
T	Test, toets, commissioning eis (te borgen in beheerfase).
B	Beheereis.
V	Verwijzing in CSR naar op te leveren bijlagen of andere documenten, registers, etc.
D	Documenteis.
IO	Input-Output qua documenten in kader van toepassing CSR.

1.3 Scope - Vastgoed Gebonden Systemen

Onder 'Vastgoed Gebonden Systemen' worden alle systemen en/of installaties verstaan die invulling geven aan functionaliteiten van het gebouw of terrein binnen de scope van de opdracht, waaronder bijvoorbeeld (niet uitputtend) systemen voor beveiliging, gebouwbeheer, (brand)veiligheid, elektro, transport, slim vastgoed en de daaraan gerelateerde netwerken en voorzieningen. Hieronder staat een niet-limitatief overzicht van voorbeelden.



BEVEILIGING	GEBOUWBEHEER	(BRAND)VEILIGHEID
Security Management Systeem (SMS)	Gebouwbeheersysteem (GBS)	Brandmeldinstallatie (BMI)
Toegangscontrolesysteem (TCS)	Klimaatbeheersing (HVAC)	Ontruimingsalarminstallatie (OAI)
Cameraobservatiesysteem (COS)	Zonwering	Sprinklerinstallatie
Intercomsysteem (ICS) [verkeer, cel]	Aansturing verlichting	Watermistinstallatie
Inbraakdetectiesysteem (IDS)	(I)IoT (multi)sensors	Blusgasinstallatie
Perimeterbeveiliging		Personen Zoek Installatie (PZI)
E-sleutelkast		Mobiele Alarm Installatie (MAI)
Vaste alarmknoppen		

OVERKOEPELEND	ELEKTRA	TRANSPORT
VGS-netwerk(en)	(Nood) Verlichting	Slagbomen
VGS-beheervoorzieningen	No break (UPS)	Bollards
VGS-monitoringsvoorzieningen	Noodstroom (NSA)	Elektrische (draai)deuren
	Energie monitoringsysteem	Speed lanes, sluizen
	Zonnepanelen	Roltrappen
	Laadpalen	Liften

Veel van deze systemen kenmerken zich als operationele technologie (OT) waar de prioriteitsstelling anders ligt dan bij informatietechnologie (IT). De veiligheid van mensen staat altijd voorop, waardoor de beschikbaarheid een hoge prioriteit vereist, gevolgd door integriteit en vertrouwelijkheid.

Er zijn vergelijkbare systemen die niet onder verantwoordelijkheid van het Rijksvastgoedbedrijf vallen. Denk hierbij aan Indoordekking/*Digital Antenna System* (DAS), C2000, facilitaire systemen, etc. Tenzij expliciet vermeld, vallen deze niet binnen de scope.

De kantoorautomatisering en/of audiovisuele voorzieningen vallen nadrukkelijk buiten dit Cybersecurity Raamwerk, deze vallen onder de verantwoordelijkheid van de ICT-dienstverlener.

1.4 Informatiebeveiliging versus Cybersecurity

Informatiebeveiliging en Cybersecurity zijn begrippen die doorgaans afwisselend gebruikt worden en waarbij in sommige definities een bepaalde nuance gegeven wordt. Binnen het RVB maken we onderscheid tussen:

- **Informatiebeveiliging bedrijfsvoering** heeft in de brede zin betrekking op de bedrijfsvoering (van Opdrachtgever, Gebruiker en Opdrachtnemer). Hiervoor geldt wet- en regelgeving (waaronder VIR, VIRBI, NIS2/Cbw) en in contracten kunnen hiervoor specifieke eisen of kaders worden meegegeven zoals de BIO en ABRO. Deze hebben qua reikwijdte zowel betrekking op de dienstverlening op een locatie als de informatiebeveiliging van de dienstverlenende organisatie zelf (Opdrachtnemer).
- **Cybersecurity Vastgoed Gebonden Systemen:** richt zich specifiek op de ‘informatiebeveiliging’ van de VGS. Dit Cybersecurity Raamwerk betreft de Cybersecurity eisen aan Opdrachtnemer over:
 - De bedrijfszekerheid en betrouwbaarheid van de VGS.
 - De beveiliging van de informatie besloten in de VGS.
 - De processen met betrekking tot de omgang met deze systemen en de daarin besloten informatie.
 - Vakbekwaamheidseisen aan medewerkers van Opdrachtnemer die met de systemen en de daarin besloten informatie omgaan.



Dit onderscheid is bewust gemaakt. Als een beheerorganisatie zijn informatiebeveiliging op orde heeft, wil dat niet persé zeggen dat de VGS die zij beheert ook cybersecure zijn en vice versa. In de praktijk zal er enig overlap kunnen zijn.

A	E1.4-01	In geval van tegenstrijdigheden geldt als uitgangspunt de zwaarst gestelde eis. De Opdrachtnemer meldt dit aan de Opdrachtgever voor een definitief uitsluitel.
---	---------	---

1.5 Cybersecurity VGS in verschillende fasen

Binnen RVB worden een aantal fasen onderscheiden in de werkwijze voor projecten:

- Definitiefase: in deze fase stelt Opdrachtgever de specificaties op en kan daarbij keuzes maken in de uitgangspunten in dit document inzake cybersecurity.
- Uitvraagfase: in deze fase wordt de opdracht in de markt gezet (inclusief dit Cybersecurity Raamwerk) voor een of meerdere van de volgende fasen, waarbij vragen gesteld kunnen worden inzake eventuele onduidelijkheden.
- Ontwerpfase: in deze fase verwerkt 'Opdrachtnemer Ontwerpfase' de cybersecurity beheersmaatregelen (eisen) in het ontwerp en verwijst ondubbelzinnig naar dit Cybersecurity Raamwerk. Eerste uitwerking van Cybersecurityplan (CSP) kunnen hier uitgewerkt worden als onderdeel van het ontwerp.
- Realisatiefase: in deze fase moet 'Opdrachtnemer Realisatiefase' de Cybersecurity van de VGS realiseren conform ontwerp en dit document. In deze fase wordt Cybersecurityplan (CSP) opgeleverd.
- Instandhoudingsfase: in deze fase moet de 'Opdrachtnemer Instandhouding' de Cybersecurity van de VGS borgen gedurende de levensduur. In het Cybersecurityplan (CSP) is vastgelegd 'hoe' dat gebeurt en wordt het document actueel gehouden.
- Afstotingsfase: bij afstoting van (een deel van) een VGS zorgt 'Opdrachtnemer Instandhouding' dat dit conform aangegeven procedures verloopt en actualiseert het CSP.

Uiteraard is de 'informatiebeveiliging' in brede zin in alle fasen geborgd conform classificatie/rubricering en overige regels op het gebied van het beveiligen van (project)informatie.

Tussen de bouwphase en instandhoudingsfase is er sprake van overdracht van het CSP. Bij ingebruikname van een systeem door Opdrachtgever of Gebruiker dient het CSP geborgd te worden door de Opdrachtnemer onder regie Opdrachtgever. Indien op dat moment de overdracht nog niet heeft plaatsgevonden, rust de verantwoordelijkheid van het CSP bij de 'Opdrachtnemer Realisatiefase'.

1.6 Wat wordt van u verwacht?

Van onze marktpartijen wordt verwacht dat zij professionele, cybersecure oplossingen bieden voor de gebouwen en haar VGS, waarbij gedegen aandacht is geschonken aan een gelaagdheid van beheersmaatregelen om risico's zoveel mogelijk te beheersen en de impact van effecten te minimaliseren. Van de Opdrachtnemer wordt vereist:

A	E1.6-01	De Opdrachtnemer conformeert zich aan de eisen in dit Cybersecurity Raamwerk (CSR) voor Vastgoed Gebonden Systemen (VGS) met inbegrip van het VGS Business Impact overzicht¹.
IO	E1.6-02	In de ontwerpfase worden de uitgangspunten en eisen van het Cybersecurity Raamwerk (CSR) in het ontwerp door Opdrachtnemer verwerkt en op diverse moment getoetst door Opdrachtgever, waar uitwerking van het Cybersecurityplan (CSP) onderdeel kunnen uitmaken.

¹ Zie Verwijzing 02: VGS Business Impact overzicht



IO	E1.6-03	- In de realisatiefase levert Opdrachtnemer het Cybersecurityplan (CSP) conform het aangereikte sjabloon² inclusief bijlagen en (al dan niet op diverse momenten) getoetst door Opdrachtgever en voor oplevering <u>ter acceptatie</u> voorgelegd. - In het CSP is uitgewerkt op welke wijze de cybersecurity-uitgangspunten en eisen zijn verwerkt in de ontwerpen van de systemen. - In het CSP is uitgewerkt 'hoe' de VGS beheerd worden, zodanig dat de <i>cybersecurity posture</i> wordt geborgd en op continue basis wordt verbeterd. - In het CSP is voor de eisen waar niet (geheel) aan wordt voldaan aangegeven dat hiervan is afgeweken. Dit met een beschrijving van de impact, een risicoclassificatie (volgens model Rijksvastgoedbedrijf), de genomen compenserende maatregelen en verwijzing naar de risicoacceptatie c.q. toestemming van de Opdrachtgever. - Het CSP is een op zichzelf staand document dat zonder verwijzingen naar andere documenten een adequaat beeld geeft 'hoe' de cybersecurity is onderbouwd en voldoende detail bevat om een audit op uit te voeren. Voor details kan verwezen worden naar plattegronden, blokschema's, functioneel ontwerp, technisch ontwerp, materiaalspecificatie, risicoanalyses en/of andere gedetailleerde gegevens.
D	E1.6-04	Het CSP worden in open format (docx) beschikbaar gesteld, zodat het eenvoudig overdraagbaar is.
D	E1.6-05	Uitgangspunt is één CSP voor beveiliging en één CSP voor alle overige VGS van het gehele complex, tenzij Opdrachtgever hier expliciet aangeeft met deelplannen te willen werken.
IO	E1.6-06	Tijdens de garantieperiode en de instandhoudingsfase en bij afstoting wordt CSP in geval van wijzigingen en/of uitbreidingen steeds geactualiseerd en beschikbaar gesteld aan Opdrachtgever voor eventuele review, zodat de actualiteit van het CSP gewaarborgd blijft.
A	E1.6-07	- Opdrachtgever behoudt het recht om periodiek en voorafgaand aan oplevering assessments en/of (technische) audits uit te (laten) voeren, waaronder bijvoorbeeld: - Een penetratietest (pen-test). - Een kwetsbaarheidscan (vulnerability scan). - Aansluiting op een <i>security operations center</i> (SOC) voor continue security monitoring.

Tijdens een project kan dit Cybersecurity Raamwerk en daaraan gerelateerd CSP worden aangepast als gevolg van wijzigingen in wet- en regelgeving of intern beleid (meest recente versie van CSR). Opdrachtgever heeft het recht om gedurende het project en/of bij oplevering op basis van een gap-analyse aanscherpingen te vereisen conform het contractuele wijzigingsproces (meerkosten).

Opdrachtgever zal in samenspraak met Opdrachtnemer Instandhouding een Cybersecurity Management Systeem (CSMS) voor VGS borgen. Het Cybersecurityplan (CSP) maken daar onderdeel van uit.

1.7 Algemene uitgangspunten

A	E1.7-01	Met betrekking tot de cybersecurity van VGS is het uitgangspunt dat deze met 'passende' beheersmaatregelen beveiligd zijn en dat u dat 'aantoonbaar' maakt, voor: - De individuele componenten en systemen. - Het samengestelde geheel van de gebouwinstallaties, koppelingen en verbindingen. - De gehele levenscyclus van de systemen en/of componenten, met een cyclische en methodische aanpak (plan-do-check-act).
---	---------	---

² Zie [VERWIJZING 01: SJABLOON CYBERSECURITYPLAN \(CSP\)](#)



A	E1.7-02	De Opdrachtnemer is verantwoordelijk voor de gehele toeleveringsketen en de daarin betrokken partijen (ontwikkeling, productie, fabricage, import, distributie, systeemintegratie, installatie, onderhoud, functioneel/technisch/applicatie beheer, ...). Daar waar er raakvlakken zijn met de cybersecurity van het geheel aan (bestaande) systemen en de locatie dienen deze geborgd te worden. Het <i>need-to-know</i> principe wordt daarbij geborgd te worden alsmede de informatiebeveiliging in brede zin conform classificatie/rubricering.
A	E1.7-03	Met ' passende ' beheersmaatregelen wordt bedoeld dat uitgegaan wordt van de op het moment van uitvraag marktconforme (gangbare) beheersmaatregelen die de kenmerkende en geïdentificeerde risico's op voldoende wijze mitigeren en in redelijkheid aanpasbaar zijn bij veranderende omstandigheden. Daarbij wordt aansluiting gezocht bij <i>best practices</i> . Hierbij speelt ook de financiële en technische haalbaarheid een rol alsmede de impact op de praktische toepasbaarheid. Eventuele restrisico's dienen altijd expliciet inzichtelijk gemaakt te worden en door de Opdrachtgever geaccordeerd te worden.
A	E1.7-04	Met ' aantoonbaar ' vereisen we dat u inzichtelijk maakt hoe invulling gegeven wordt aan de beheersmaatregelen en hoe dit geborgd wordt. Denk hierbij aan: • Expliciete instemming met de gestelde vereisten van dit document en toelichting als er niet of slechts gedeeltelijk ingestemd kan worden ('pas toe of leg uit') in het CSP. • Uitwerking in een CSP hoe de beheersmaatregelen voor de verschillende systemen samenkomen en nadere toelichting daarop. • Overleggen van certificeringen, auditrapportages en/of bewijs van bekwaamheid. • Geplande follow-up acties aangaande de bevindingen in auditrapportages inclusief <i>roadmap</i>.

Opdrachtgever wil hierbij inzage in de volledige documentatie om een goed beeld van de **scope** en reikwijdte te verkrijgen en vraagt de Opdrachtnemer dit op voorhand expliciet kenbaar te maken. Voorgaande set van documentatie dient de basis te vormen van het beheer van de maatregelen gedurende de gehele levenscyclus.



1.8 Wet- en regelgeving, normenkaders en benchmarks

In Nederland zijn in het kader van Cybersecurity voor VGS de meest relevante wetten:

- **Network and Information Security directive (NIS2³) > Cyberbeveiligingswet (Cbw)**
Cybersecurity richtlijn voor essentiële en belangrijke entiteiten. De Cbw is vanaf 15 augustus 2026 van kracht.
- **Cyber Resilience Act (CRA)⁴**
Security by design en default van digitale producten, software bill of materials (SBOM), meldplicht inzake kwetsbaarheden, waarbij gedurende (technische) levensduur ondersteuning inzake kwetsbaarheden gegeven moet worden. Eind 2027 volledige van kracht, meldplicht is vanaf september 2026 van kracht. Gericht op fabrikanten, importeurs en distributeurs. Van toepassing op alle VGS.
- **Radio Equipment Directive (RED)⁵**
Eisen aan radioapparatuur incl. cybersecurity. Van kracht sinds 2025. Van toepassing op WiFi, Bluetooth, Zigbee, LTE/5G, LoRa, radio frequenties, draadloze sensoren, etc.
- **General Data Protection Regulation (GDPR) > Algemene Verordening Persoonsgegevens (AVG)⁶**
Verwerking, omgang en beveiliging van persoonsgegevens. Van kracht sinds 2019. Van toepassing op VGS waar persoonsgegevens verwerkt worden, zeker relevant voor cameratoezicht, toegangscontrole, registratie bezoekers, biometrie, laadpalen, bezetting- en reserveringsystemen, mobiele apps voor bediening, etc.
Indien er persoonsgegevens verwerkt worden die het primaire proces van de Gebruiker raken, kan aanvullende privacywetgeving van toepassing zijn (bijv. Wet justitiële en strafvorderlijke gegevens (WJSG) inzake justitie).
- **Artificial Intelligence Act (AIA)**
Regels voor AI-systemen o.b.v. risico. Gefaseerde invoering 2025-2027. Van toepassing op gebruik van AI voor VGS en/of in clouddiensten. Bijvoorbeeld analyse camerabeelden, AI optimalisatie klimaatbeheersing).
- **Cyber Security Act (CSA)**
Europees cybersecurity-certificeringskader. Van kracht sinds 2019. Van toepassing op ICT-producten en diensten.
- **Data Act (DA)**
Regels rond toegang/deling van IoT-data voor fabrikanten en cloudproviders. Grotendeels van kracht sinds 2025. Relevant voor VGS inzake uitlezen data, overdraagbaarheid, interoperabiliteit en wisselen van cloudprovider.
- **Critical Entities Resilience Directive (CER) > Wet weerbaarheid kritieke entiteiten**
Weerbaarheid van kritieke entiteiten. Van kracht sinds 2024. Specifiek voor aangewezen sectoren, enkel relevant voor vitale gebouwen/infrastructuur/datacenters.

³ NIS2/Cbw: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/>

⁴ CRA: <https://www.european-cyber-resilience-act.com/>, <https://www.rdi.nl/documenten/2025/09/19/gids-cyber-resilience-act>

⁵ RED: <https://www.rdi.nl/onderwerpen/draadloze-apparatuur/handel-en-apparatuur>

⁶ AVG: <https://wetten.overheid.nl/BWBR0040940/2021-07-01>



Binnen de Rijksoverheid zijn onderstaande besluiten en kader met name relevant inzake cybersecurity van vastgoed gebonden systemen:

- Voor de Rijksoverheid
 - **VIR-2007**⁷: Besluit voorschrift informatiebeveiliging rijksdienst 2007
 - **VIRBI 2025**⁸: Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2025
 - **BIO2**: Baseline Informatiebeveiliging Overheid versie 2 (2025), hierna te noemen **BIO**⁹ t.a.v. informatiebeveiliging, hetgeen onverminderd van toepassing is op VGS in en op haar vastgoed.
 - **ABRO**¹⁰: Algemene Beveiligingseisen voor Rijksoverheidsopdrachten
Vanaf 1 januari 2026 gelden nieuwe beveiligingseisen voor bedrijven die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid.
- Voor Defensie:
 - Het Defensie Beveiligingsbeleid (DBB)¹¹
 - De BIO is opgenomen in de D/301 en in de D/302 staan aanvullende eisen inzake informatiebeveiliging in geval van Dep.V en hogere rubriceringen¹².

In dit Cybersecurity Raamwerk voor VGS zijn de beheersmaatregelen uit voorgaande wetten en normenkader vertaald naar de vastgoed context.

De toepassing van het Cybersecurity Raamwerk Vastgoed Gebonden Systemen en het Cybersecurityplan (CSP) is staand beleid van het Rijksvastgoedbedrijf.

A	E1.8-01	• Alle Vastgoed Gebonden Systemen in scope van de opdracht voldoen aan de eisen gesteld in dit Cybersecurity Raamwerk.
A	E1.8-02	• De ABRO is van toepassing op bedrijven die voor de overheid een opdracht uitvoeren met risico's voor de nationale veiligheid (te beschermen belangen 4 t/m 1) en/of daar waar het gaat om gerubriceerde informatie (Departementaal Vertrouwelijk of hoger).

⁷ VIR: <https://wetten.overheid.nl/BWBR0022141/2007-07-01>

⁸ VIRBI: <https://wetten.overheid.nl/BWBR0051482/2025-09-09/0>

⁹ BIO: <http://www.bio-overheid.nl/>

¹⁰ ABRO: <https://www.rijksoverheid.nl/onderwerpen/zakendoen-met-het-rijk/beveiligingseisen-abro>

¹¹ DBB: het Defensie beveiligingsbeleid is niet openbaar.

¹² Defensienormen D/301 en D/302 zijn niet openbaar



2 RISICOMANAGEMENT & CLASSIFICATIE VGS EN DATA

2.1 Classificatie/Rubricering

Deze paragraaf behandelt de classificatie/rubricering van locaties, ruimten, netwerken, systemen en gegevens in en over VGS.

VGS kunnen vertrouwelijke gegevens bevatten, die conform classificatie en/of rubricering terdege beschermd moet zijn. Denk hierbij aan:

- Plattegronden en benamingen specifieke ruimtes
- Zwakke plekken in beveiliging locatie
- Systeemdokumentatie
- Systeem en softwareversies
- Kwetsbaarheden in de systemen
- Persoonsgegevens¹³
- Etc.

De VGS zelf kunnen ook geclassificeerd worden en/of in een ruimte worden toegepast van een bepaalde classificatie.

- Van rubricering is sprake als informatie geduid wordt als Departementaal Vertrouwelijk of Staatsgeheim, van classificatie is sprake als informatie wordt als Openbaar, Intern Algemeen of Intern Vertrouwelijk.¹⁴
- Alle locaties, systemen en data – alsmede de documentatie daaromtrent – worden door Opdrachtgever geclassificeerd/gerubriceerd en eventueel van merking voorzien.
- Classificaties en/of rubriceringen worden door Opdrachtgever vastgelegd in bijvoorbeeld een Classificatie- (CAL) of Rubriceringsaanduidingslijst (RAL).

A	E2.1-01	• Indien géén classificatie is toegekend aan een locatie, systeem, gegevens of de documentatie daaromtrent verzoekt Opdrachtnemer Opdrachtgever een classificatie toe te kennen. Totdat uitsluitel is gegeven wordt minimaal uitgegaan van classificatie 'Intern Vertrouwelijk'.
A	E2.1-02	• Indien Opdrachtnemer een nieuw document vervaardigt, dient Opdrachtnemer dit te classificeren of rubriceren in overleg met Opdrachtgever of de daartoe aangewezen Rubriceringsambtenaar.
A	E2.1-03	• Derubricering, pseudonimisering en/of anonimisering dienen in goed overleg met de Opdrachtgever plaats te vinden en vereisen schriftelijk akkoord voor zowel de gebruikte methode als het specifieke gebruik van de data: Welke data wordt waarom en hoe gepseudonimiseerd en/of geanonimiseerd.
A	E2.1-04	• Alle geclassificeerde/gerubriceerde informatie en bedrijfsmiddelen/VGS die dergelijke informatie bevatten zijn gelabeld volgens het door Opdrachtgever vastgestelde classificatie- en/of rubriceringsschema.

¹³ Zie §0

VERWERKING VAN persoonsgegevens

¹⁴ Zie 0 BIJLAGE B : Rubriceringsmatrix voor kenmerken van de verschillende rubriceringen en classificaties.



2.2 Risicomanagement / Business impact analyse VGS

Alle systemen en netwerken en de daarin besloten informatie worden door middel van een expliciete risicoafweging geïnclassificeerd. Hierbij wordt gebruik gemaakt van een vastgestelde classificatiemethodiek die onderdeel is van de vastgestelde risicomanagementmethodiek.

Opdrachtgever is in samenspraak met Gebruiker verantwoordelijk voor de classificatie, impactbepalingen en/of risicoanalyses. Opdrachtnemer participeert proactief in dit proces.

Specifieke ontwerpkeuzes zoals al dan niet externe toegang en/of cloudtoepassingen, specifieke toepassingen van ruimtes, etc. zorgen voor aanvullende nuances in de risicoafweging.

Verwijzing 04: Instructie classificatie VGS

- Opdrachtgever stelt overzicht van VGS en bijbehorende classificatie beschikbaar.
- **Locaties en/of ruimtes** worden door Opdrachtgever geïnclassificeerd op basis van 0 'Bijlage B : Rubriceringsmatrix'.
- **Vastgoed Gebonden Systemen** worden door Opdrachtgever in samenspraak met Gebruiker geïnclassificeerd op basis van:
 - **BIV** vanuit het perspectief van de Gebruiker
 - **Beschikbaarheid** in termen van toegankelijkheid, continuïteit en robuustheid
 - **Integriteit** in termen van betrouwbaarheid, juistheid, volledigheid, actualiteit en tijdigheid.
 - **Vertrouwelijkheid** op basis van 0 'Bijlage B : Rubriceringsmatrix'.
 - **Impact** vanuit het perspectief van de Gebruiker
 - Verstoring continuïteit **primaire proces / Te Beschermen Belangen**
 - **Veiligheid** van mensen in gevaar
 - **Financiële** (economische) en/of herstelschade (materiële schade)
 - **Imago en politieke** schade (immateriële schade)

De impact-weging dient nader afgestemd te worden, zie voorzet onderstaande tabel.

Impact	Primaire proces/TBB	Veiligheid mensen	Financieel	Imago / politiek
1 Laag	Meerdere klachten werkomstandigheden	Gewonde zonder blijvend letsel/kort verzuim (<2w)	< € 50k	• Lokale commotie • Escalatie management
2 Gemiddeld	Ernstige klachten, risico op verstoring proces of TBB's	<5 gewonden met blijvend letsel/langdurige verzuim	< € 250k	• Regionale commotie • Escalatie directie
3 Hoog	Primaire proces ernstig verstoord, >25% en > 1 week.	<10 gewonden met blijvend letsel	< € 1 M	• Landelijke commotie • Escalatie DG/SG
4 Kritiek	Primaire proces gebruiker volledig verstoord	doden of > 10 gewonden met blijvend letsel	> € 1 M	• Internationale commotie • Tweede Kamer vragen

A	E2.2-01	• Opdrachtnemer participeert proactief in het proces van classificatie, impactbepaling en/of risicoanalyse.
R	E2.2-02	• Opdrachtnemer registreert uitkomsten van classificatie, impact- en/of risicoanalyses in door Opdrachtgever aangewezen informatiesystemen (zoals assetmanagement systeem, risicoregister).
R	E2.2-03	• Opdrachtnemer ondersteunt actief in risicoafhandeling: informeert omtrent (rest)risico's en implementeert risico mitigerende maatregelen die door Opdrachtgever (Gebruiker) zijn goedgekeurd. Dit omvat minimaal: - Signalering van alle afwijkingen t.a.v. het risicoregister. - Motivatie van alle afwijkingen - Doornemen van afwijkingen met Opdrachtgever.

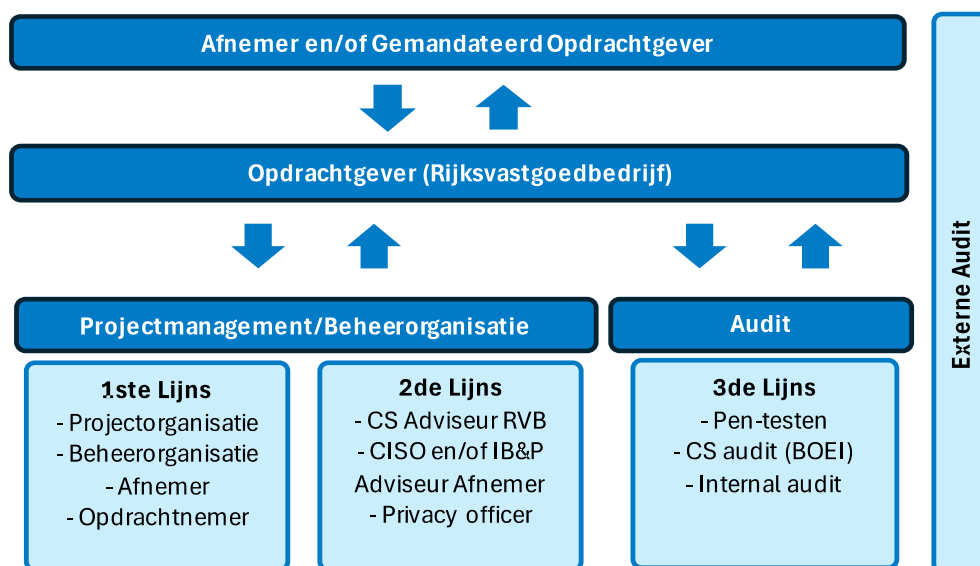


	- Uitvoering van mitigerende maatregelen op basis van een risico-inschatting - Afhandeling van restrisico's volgens daartoe vastgestelde procedure: ▪ Een laag restrisico kan worden geaccepteerd door Opdrachtgever (let op cumulatieve risico's). ▪ Bij een hoog restrisico is een door Opdrachtgever (in geval Kantorenstelsel) en/of Gebruiker (in geval (Bijzondere) <i>Specialty</i> stelsel of Defensie) afgetekende risico-acceptatie verplicht.
--	---

2.3 Risicodossier / Compliance

B	E2.3-01	• De Opdrachtnemer onderhoudt voor elke locatie een Cybersecurityplan (CSP) waarin voor elk Vastgoed Gebonden Systeem in beheer de mate van conformiteit aan de normen uit het Cybersecurity Raamwerk (CSR) met een onderbouwing is geregistreerd.
B	E2.3-02	• De Opdrachtnemer onderhoudt voor elke locatie een Risicodossier en registreert daarin de risico's verbonden aan de CSR-normen waaraan niet wordt voldaan.
B	E2.3-03	• De opdrachtnemer stelt voor elk Hoog en/of Kritiek risico een Verbeterplan op en stemt dit af met Opdrachtgever.

- Risicomanagement wordt vormgegeven o.b.v. het *Three Lines of Defense*-model
 - Eerstelijns rollen is de project- of beheerorganisatie bestaande uit Opdrachtgever, Gebruiker, CDV, Opdrachtnemer.
 - Tweedelijns rollen zijn vanuit specifieke expertises betrokken.
 - Derdelijns rollen zijn vanuit onafhankelijk (intern) auditperspectief. Dit kan ook gaan over (periodieke) pen-testen vanuit Opdrachtgever.





2.4 Verwerking van persoonsgegevens

Bij operationele technologie draait het primair om veiligheid en beschikbaarheid, maar o.a. cameratoezicht, toegangscontrole, security management, biometrische toepassingen, personenzoekinstallaties/mobielalarminstallaties en gespreksopnames bevatten de nodige (bijzondere) persoonsgegevens. Ook bij smart building concepten of bij combinaties van bepaalde informatiebronnen zijn vaak (herleidbare) persoonsgegevens betrokken waarop de Algemene Verordening Gegevensbescherming (AVG) van toepassing is.

Opdrachtgever geeft in haar specificatie – daar waar mogelijk – aan welke persoonsgegevens in welke specifieke VGS verwerkt mogen worden en/of welke juist niet.

R	E2.4-01	Opdrachtnemer maakt in het CSP inzichtelijk welke gegevens(velden) in Vastgoed Gebonden Systeem opgeslagen zijn alsmede de gegevens die tussen systemen wordt uitgewisseld.
---	---------	---

Opdrachtgever draagt zorg voor afstemming met een privacy officer of functionaris gegevensbescherming (FG) inzake de inventarisatie persoonsgegevens en al dan niet benodigde *Data Privacy Impact Assessment* (DPIA). Opdrachtgever verwerkt de uitkomsten hiervan in een verwerkersovereenkomst die met Opdrachtnemer wordt aangegaan.

A	E2.4-02	Opdrachtnemer gaat een verwerkersovereenkomst met Opdrachtgever aan, als sprake is van verwerking van persoonsgegevens van Opdrachtgever door Opdrachtnemer.
A	E2.4-03	- Opdrachtnemer biedt volledig inzicht in de keten van verwerkers van persoonsgegevens en de van toepassing zijnde verwerkersovereenkomsten. - Opdrachtnemer borgt verwerkingsverantwoordelijkheden in de toeleveringsketen.
A	E2.4-04	Persoonsgegevens en vertrouwelijke gegevens verlaten de locatie nooit zonder expliciete, schriftelijke toestemming van Opdrachtgever.
A	E2.4-05	Persoonsgegevens en vertrouwelijke gegevens worden met passende beheersmaatregelen beschermd. Dergelijke gegevens dienen te allen tijde versleuteld te worden opgeslagen en verstuurd met daartoe geschikte versleutelingsstandaarden. Dergelijke gegevens worden bij voorkeur enkel lokaal opgeslagen en/of binnen Nederland, doch altijd binnen de grenzen van de Europese Unie.

2.5 Beschermen registraties en Bewaartermijnen

A	E2.5-01	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.
O	E2.5-02	Opslagvoorzieningen hebben afdoende capaciteit om aan de gestelde bewaartermijnen te voldoen. Uitbreiding van de opslagcapaciteit is mogelijk. De <i>Time To Live</i> (TTL) van opgeslagen gegevens is flexibel instelbaar.
A	E2.5-03	Wettelijke en overeengekomen minimale en maximale bewaartermijnen van gegevens zijn geborgd. Bewaartermijnen - De bewaartermijnen zijn van toepassing op alle log-data en op applicatie-data op het moment dat deze inactief wordt (bijvoorbeeld op het moment dat een toegangspas uit het systeem verwijderd wordt).



	- Lokaal endpoint: voor lokaal vastgelegde log-gegevens (op <i>endpoint devices</i> als camera's, intercoms, deurcontrollers) geldt een bewaartermijn van <u>minimaal 6 maanden</u>. Indien de log-gegevens volledig naar een applicatieserver worden gekopieerd, kan de maximale bewaartermijn op het endpoint teruggebracht worden naar 7 kalenderdagen. - Applicatie: voor loggegevens en inactief geworden gegevens op servers (centrale applicatie) en/of client pc's t.b.v. beheer, bediening, besturing voor het specifieke systeem geldt een bewaartermijn van <u>(minimaal en maximaal) 3 jaar</u>. Indien de data naar een rapportagevoorziening wordt gekopieerd, kan dit teruggebracht worden naar <u>1 jaar</u>. Dit is zowel relevant voor onderzoeken bij incidenten als mogelijke (trend)analyses/rapportages. - Rapportage: hiermee wordt bedoeld dat de (log)gegevens gekopieerd wordt naar een centrale management-, log- en/of rapportageserver voor analyse en rapportagedoeleinden. Hier geldt dat over een periode <u>van 3 jaar</u> analyses en rapportages mogelijk moeten zijn. - Met betrekking tot camerabeelden geldt een bewaartermijn van (minimaal en maximaal) 28 dagen. - Specifiek geselecteerde camerabeelden kunnen worden uitgezonderd van overschrijven of wissen (bijvoorbeeld voor onderzoek en/of bewijsvoering bij incidenten totdat deze veilig gesteld worden). Uitgangspunt is dat opslag van deze beelden niet meer dan 1% van de totale opslagcapaciteit voor camerabeelden in beslag nemen. • Data van security incidenten dienen minimaal 3 jaar bewaard te worden (en indien Staatsgeheim minimaal 5 jaar), waarbij het uitgangspunt is dat deze informatie binnen uiterlijk 3 maanden moet zijn veiliggesteld buiten de VGS.
--	--

2.6 Eigendom gegevens

Gegevens zijn steeds belangrijker bij aansturing van systemen in gebouwen en vormt een centraal onderdeel in de digitalisering. Voor Opdrachtgever is het van belang dat zij in control blijft over deze gegevens en dat de vertrouwelijkheid, integriteit en beschikbaarheid wordt geborgd.

A	E2.6-01	• Opdrachtgever blijft te allen tijde eigenaar van de gegevens die zich in de systemen bevindt of hierin wordt gegenereerd, dan wel in andere systemen worden verwerkt (in oorspronkelijke en bewerkte vorm). Opdrachtgever dient expliciet toestemming te verlenen voor verwerking van gegevens, toegang tot die gegevens en/of het delen met derden.
---	---------	---

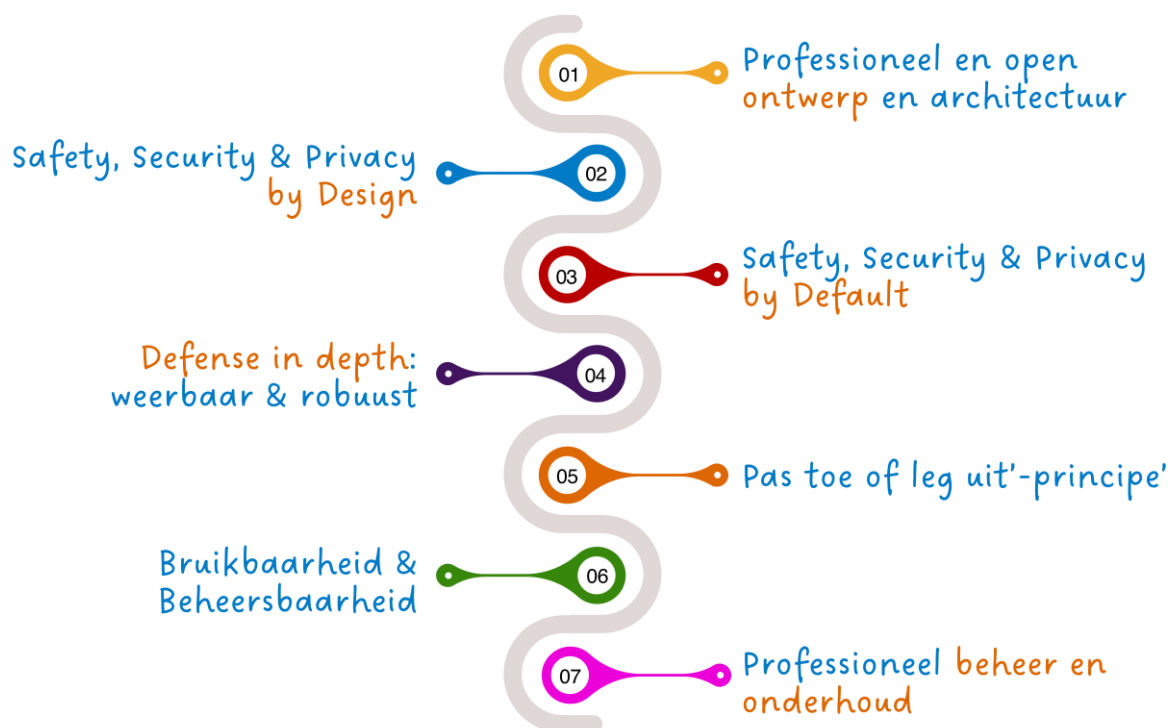
3 PRINCIPES & ARCHITECTUUR

3.1 Visie en beleid

A	E3.1-01 Opdrachtnemer beschrijft kort en bondig in het CSP haar visie en beleid op het gebied van cybersecurity inzake de scope van de opdracht, met in het bijzonder aandacht voor: • Ontwerpen en realiseren van een veilig systeem, netwerk en koppelvlakken • De samenwerkende partijen in de toeleveringsketen en de borging van cybersecurity in deze samenwerking, • Vormgeving van de ondersteuning van uw product gedurende de levensduur.
---	--

3.2 Principes

Een aantal **principes**¹⁵ liggen ten grondslag aan cybersecure maatregelen voor VGS, waarvan vereist wordt dat die in de gehele oplossing terugkomen.



P3.2-01 A	• <i>Professioneel en open ontwerp en architectuur</i> De netwerken en systemen worden conform best practices op een professionele manier ontworpen in lijn met open architectuur uitgangspunten en de te beschermen belangen. Het ontwerp is transparant en open: er worden open standaarden gebruikt en er zijn géén <i>Black boxes</i>.
P3.2-02 A	• <i>Safety, Security & Privacy by Design</i> In het ontwerp worden veiligheid, beveiliging en privacy geborgd. De prioritering van deze aspecten is context-afhankelijk, en wordt eenduidig inzichtelijk gemaakt. - Externe verbindingen en netwerken zijn altijd <i>Secure-by-Design</i>.

¹⁵ Gebaseerd op: 'Security Architecture: Navigating complexity', maart 2021 en 'Industrial Control Systems: Security Controls Guide' december 2019, beide van Information Security Forum (ISF) en Baseline Informatiebeveiliging Overheid (BIO).



	- Bij VGS staat (indien relevant in de context) veiligheid voorop. • Het ontwerp moet ter toetsing en goedkeuring worden voorgelegd aan Opdrachtgever.
P3.2-03 A	• <i>Safety, Security & Privacy by Default</i> Bij de daadwerkelijke inrichting/configuratie van VGS zijn de meest veilige en best beveiligde opties als uitgangspunt genomen die de minste impact hebben op de privacy. Hierbij wordt de haalbaarheid meegewogen en staat veiligheid wederom voorop. Hiervoor geldt ook dat bewuste afwegingen (met Opdrachtgever) per onderdeel gemaakt worden, waarop wordt teruggevallen bij verstoringen: 'fail safe' versus 'fail secure' en/of 'default allow' versus 'default deny'.
P3.2-04 A	• <i>Defense in depth: weerbaar & robuust</i> Beheersmaatregelen zijn vormgegeven volgens het principe van gelaagde, samenhangende beveiliging, teneinde weerbare en robuuste VGS te realiseren. Er is zorgvuldig nagedacht hoe organisatorische, technische/logische en fysieke maatregelen elkaar versterken. Alsmede hoe deze maatregelen de oorzaak mitigeren met voorzorgsmaatregelen en het effect beperken middels tegenmaatregelen. Daar waar ze niet toereikend zijn kunnen compenserende maatregelen worden voorgesteld om de risico's alsnog voldoende te mitigeren. DEFENSE IN DEPTH ORGANISATIE & MENS TECHNISCH en LOGISCH FYSIEKE BEVEILIGING DIRECTIEF AFSCHRIKKEN PREVENTIEF DETECTIEF CORRECTIEF HERSTEL COMPENSATIE VOORZORGS- & TEGENMAATREGELEN
P3.2-05 A	• <i>'Pas toe of leg uit'-principe</i> ('comply or explain') Uitgangspunt is dat aan alle gestelde beheersmaatregelen (eisen) wordt voldaan ('pas toe'). Het kan voorkomen dat bepaalde eisen niet relevant zijn of dat er voor bepaalde situaties/onderdelen specifiek van afgeweken moet worden. Die gevallen zijn dan onderbouwd ('leg uit') voorgelegd ter goedkeuring aan Opdrachtgever. Het is daarbij van belang het gevraagde beveiligingsniveau zo goed mogelijk te benaderen met andere en/of compenserende maatregelen. De afwijkingen zijn expliciet vastgelegd en onderdeel van een periodieke monitor, teneinde na te kunnen gaan hoe de maatregel op een later moment alsnog op het gewenste niveau gebracht wordt.
P3.2-06 A	• <i>Bruikbaarheid & Beheersbaarheid</i> Bij het ontwerpen en realiseren van de beheersmaatregelen is het van belang dat zaken niet onnodig complex worden, maar dat de oplossing bruikbaar- en beheersbaar blijft. Kortom, is een beheersmaatregel haalbaar in termen van financiën, techniek, gebruiksgemak en de beheerorganisatie.
P3.2-07 A	• <i>Professioneel beheer en onderhoud</i> Cybersecurity staat of valt bij een accuraat beheer conform uitgangspunten. Professioneel ICT-beheer is bijvoorbeeld volgens ITIL-processen vormgegeven (of wordt als zodanig overgedragen), zodat op basis van <i>best practices</i> alle processen voldoende invulling krijgen. Denk hierbij specifiek aan informatiebeveiliging, assetbeheer, wijzigingenbeheer, configuratiemanagement, <i>life-cycle</i> management, patchmanagement, incidentmanagement en bedrijfscontinuïteit, maar vooral ook aan training en bewustwording.

3.3 Scope en blauwdruk van de netwerk- & systeemarchitectuur

E3.3-01 A	Alle Vastgoed Gebonden Netwerken, Systemen en de Koppelvlakken die hierbinnen gerealiseerd worden, vallen binnen de scope van dit Raamwerk. Opdrachtnemer stelt alle betrokken leveranciers en system integrators hier expliciet van in kennis.
--------------	---



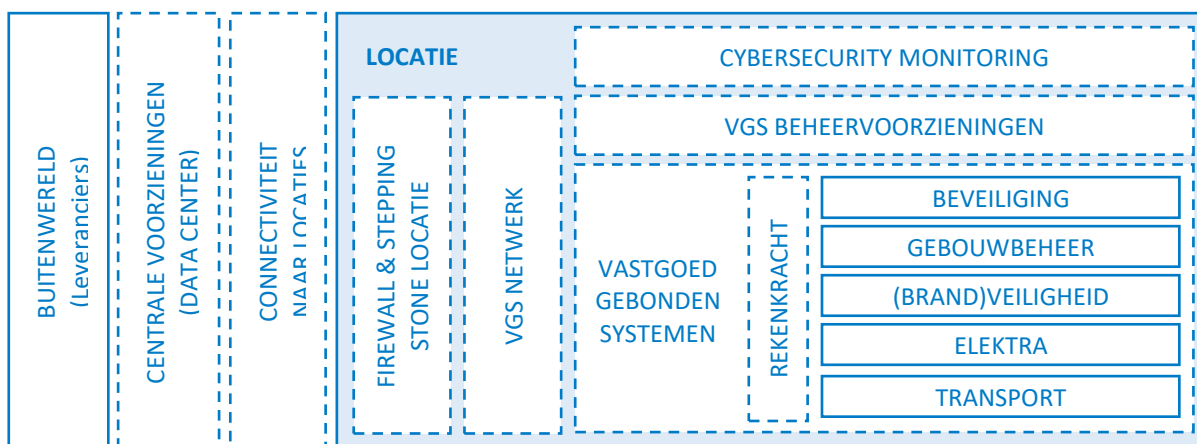
D	E3.3-02 De leveranciers, system integrators, fabricaten, merken zijn volgens het schema in het CSP inzichtelijk gemaakt.
---	---

3.4 VGS CS Referentiearchitectuur (CSRA)

De voorgestelde architectuur, netwerk- & serverinfrastructuur en dienstverlening zijn toekomstbestendig. Dat wil zeggen dat het op locatie in lijn met de VGS Cybersecurity Referentiearchitectuur (CSRA) ontworpen is, schaalbaar is en gekoppeld kan worden aan locatie-overstijgende VGS-beheer en monitoring voorzieningen (in de toekomst o.b.v. centrale connectiviteit en voorzieningen in een datacenter).

Opdrachtgever is gerechtigd op termijn onderdelen als Cybersecurity Monitoring, VGS-netwerk, VGS-beheervoorzieningen, *firewall & stepping stone* en/of servercapaciteit (rekenkracht) te centraliseren en standaardiseren bij door Opdrachtgever aangewezen partijen.

De VGS-Architectuur kent de volgende globale indeling.



Binnen het Rijksvastgoedbedrijf is de VGS Cybersecurity Referentiearchitectuur volop in ontwikkeling. Daar waar mogelijk kunnen specifieke bouwblokken beschikbaar gesteld worden.

A	E3.4-01 De VGS Cybersecurity Referentiearchitectuur wordt toegepast in het geval van nieuwbouw en renovatieprojecten en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...) op aangeven van Opdrachtgever. Op aangeven van Opdrachtgever en/of in overleg met Opdrachtnemer zijn afwijkingen en hybride varianten bespreekbaar.
A	E3.4-02 Opdrachtnemer belegt en borgt in het kader van de VGS Cybersecurity Referentiearchitectuur specialistische expertise bij (vak)bekwame en geschikte dienstverleners die betrokken worden bij het ontwerp, de realisatie en die in staat zijn de eerste 5 jaar na oplevering marktconform invulling te geven aan de gevraagde dienstverlening. In dit documenten worden deze partijen aangeduid als: - Managed Service Provider (MSP), verantwoordelijk voor de inrichting van de netwerkinfrastructuur, externe connectiviteit, server en client infrastructuur, VGS-beheervoorzieningen en health monitoring. - Security Operations Center (SOC) verantwoordelijk voor de security monitoring in de brede zin van het woord.



<u>A</u> <u>E3.4-03</u>	Opdrachtnemer werkt aan een toekomstbestendige VGS-architectuur op basis van de volgende uitgangspunten: • Uniformering en centralisering, waar mogelijk, van VGS-netwerkvoorziening binnen gebouw(en) en campus (H4 NETWERKARCHITECTUUR & VERBINDINGEN). • Centrale, overkoepelende VGS-beheervoorzieningen. • Centrale, overkoepelende VGS health monitoringsvoorzieningen door MSP (§7.4 Health Monitoring) • Centrale, overkoepelende VGS cybersecurity monitoringsvoorzieningen door SOC (§7.3 Security Monitoring). • Bundelen rekenkracht VGS waar mogelijk. • Verantwoorde, veilige externe connectiviteit middels firewall en stepping stone (indien externe connectiviteit is toegestaan) (§4.6 Externe Connectiviteit – Vereisten). • Externe connectiviteit moet vervangbaar zijn door ‘Rijks’-connectiviteit. • Het moet mogelijk zijn om de buitenwereld via een door het Rijksvastgoedbedrijf aangewezen datacenter te laten verlopen.
A <u>E3.4-03E3.4-04</u>	VGS Leveranciers sluiten aan op de CSRA, waaronder: • Netwerkinfrastructuur. • Beheervoorzieningen. • Server (compute) infrastructuur om VGS applicaties virtueel. • Security & health monitoring integratie. Uitsluitend met expliciete goedkeuring Opdrachtgever wordt hiervan afgeweken.
A <u>E3.4-04E3.4-05</u>	• Voordat de Opdrachtnemer een MSP en SOC-dienstverlener contracteert, beoordeelt de Opdrachtgever de bekwaamheid en geschiktheid van de voorgestelde dienstverlener. De Opdrachtgever kan daarnaast voorschrijven dat gebruik wordt gemaakt van een specifieke SOC en/of MSP-dienstverlener, bijvoorbeeld op grond van rijksbrede raamovereenkomsten, dan wel bepalen dat de SOC en/of MSP-dienstverlening geheel of gedeeltelijk wordt uitgevoerd door een SOC en/of MSP (ICT Dienstverlener) van de Rijksoverheid.
A <u>E3.4-05E3.4-06</u>	• De netwerk- en serverinfrastructuur, de security monitoring en de beheervoorzieningen worden zodanig ontworpen, ingericht en gedocumenteerd dat het beheer daarvan gedurende de levensduur geheel of gedeeltelijk kan worden overgedragen aan een door de Opdrachtgever aangewezen MSP en/of SOC-dienstverlener, zonder ingrijpende technische wijzigingen of afhankelijkheid van de Opdrachtnemer.

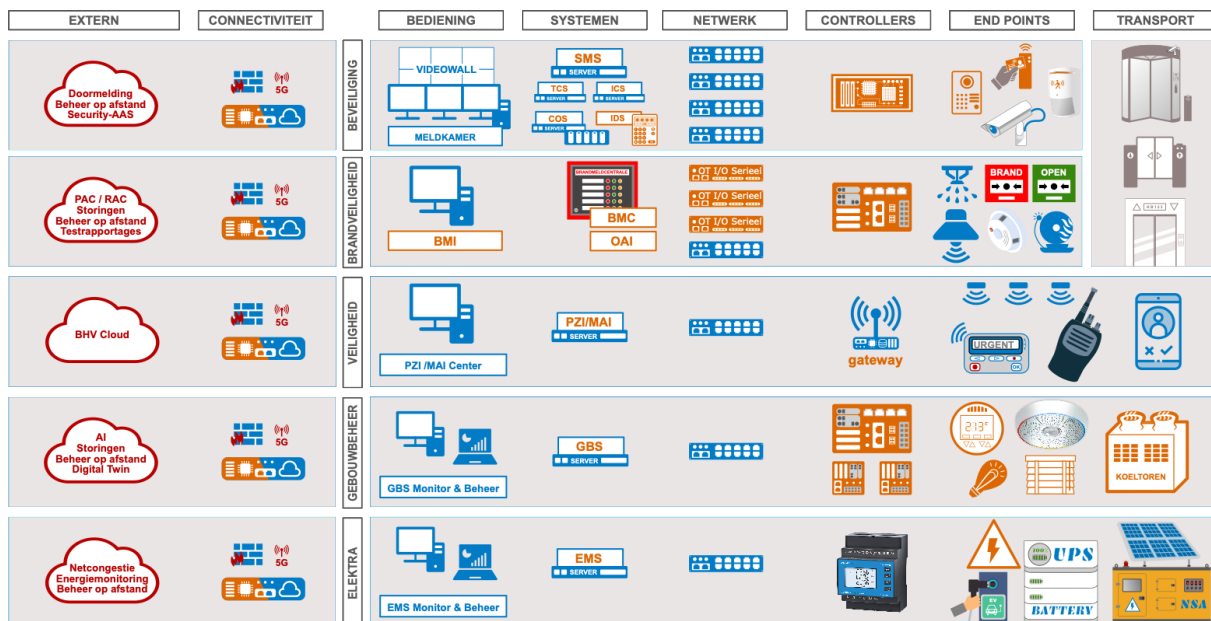
Onder ‘Centrale, overkoepelende VGS-beheervoorzieningen’ worden alle deelbare voorzieningen – zoals in dit document beschreven – voorzien, alsmede mogelijkheden om data extern te ontsluiten. Denk hierbij aan: logisch toegangsbeheer via Active Directory, NAC, certificaatbeheer, back-up, tijdssynchronisatie, etc.

Onder ‘Bundelen rekenkracht VGS waar mogelijk’ wordt de server- en storage infrastructuur verstaan waarop zowel beheervoorzieningen, als security monitoring als de VGS applicaties zelf virtueel kunnen landen.

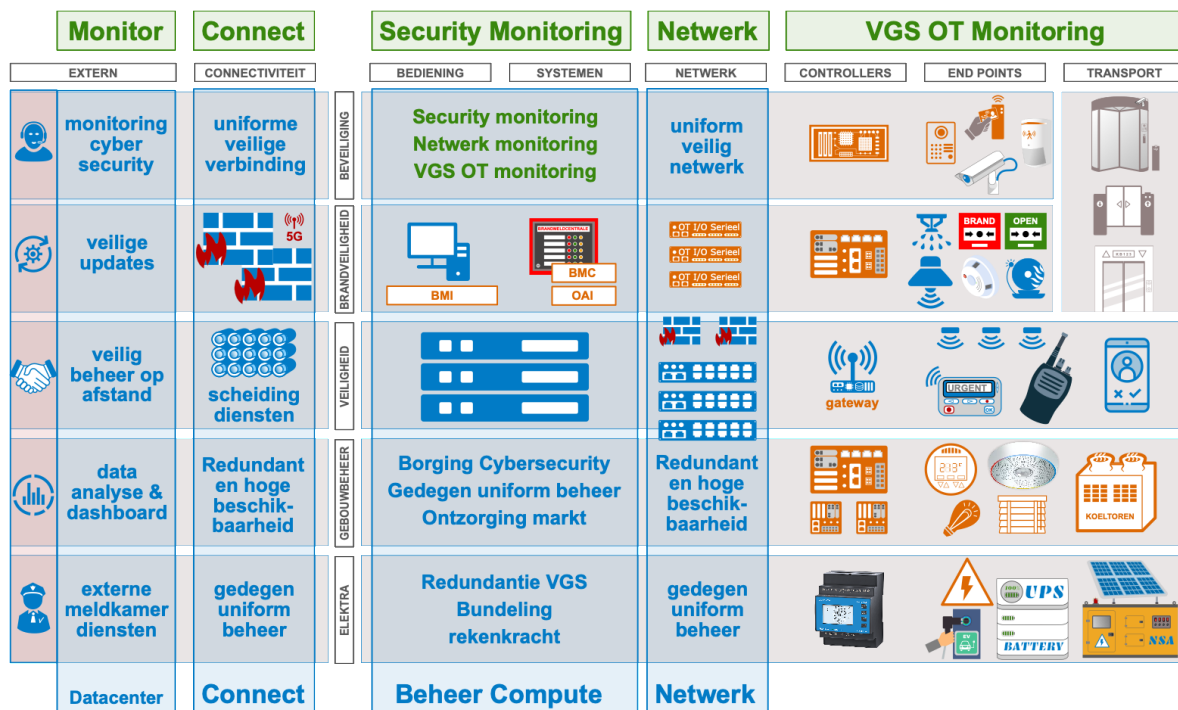
Onderstaand figuur geeft een globaal beeld hoe onderscheid gemaakt kan worden in de gelaagdheid van systemen.



Fout! Verwijzingsbron niet gevonden.



Onderstaande figuur visualiseert mogelijke optimalisaties.





3.5 Blauwdruk – high- & low-level design

A	E3.5-01 Opdrachtnemer werkt een blauwdruk uit – initieel in de vorm van een <i>High-Level Design</i> – hetgeen: • Een duidelijk beeld en overzicht geeft van alle VGS in scope en hun componenten op hoofdlijnen. • Inzicht geeft in koppelvlakken tussen VGS en/of componenten zowel binnen de scope als daarbuiten. • Inzicht te geven in ontwerpkeuzes en geschikt te zijn voor een risicoanalyse op hoog niveau. • Een overzicht bevat van de belangrijkste cybersecurityeisen.
A	E3.5-02 Opdrachtnemer werkt in volgende fasen van het project de ontwerpen meer gedetailleerd uit (<i>Low Level Design, LLD</i>). Ook afwijkingen van cybersecurityeisen worden in het LLD gedocumenteerd.

3.6 Landen met een actief offensief cyberprogramma tegen Nederland

A	E3.6-01 Leveranciers, producten of diensten uit landen met een actief offensief cyberprogramma dat gericht is tegen Nederlandse belangen zijn uitgesloten, voor: • Beveiligingssystemen (ABRO 3.3.1). • Alle elektronische apparatuur in een Stg. omgeving (ABRO 3.3.27). • Alle beveiligingsmechanismes (zijnde cybersecurity oplossingen) (ABRO 4.5.8). • Online (cloud)diensten (ABRO 5.1.3). • Producten/diensten die kritisch zijn voor het nationaal belang. op basis van de C2000-criteria: • De partij die de dienst of product levert is afkomstig, of staat onder controle van een partij, uit een land met wetgeving die commerciële of particuliere partijen verplicht samen te werken met de overheid van dat land, in het bijzonder met staatsorganen die zijn belast met een inlichtingen- of militaire taak, of is de partij een staatsbedrijf. • De partij die de dienst of product levert is afkomstig uit een land met een actief offensief inlichtingenprogramma gericht op Nederland en Nederlandse belangen of een land waarmee de Nederlandse relatie dusdanig gespannen is dat acties die Nederlandse belangen aantasten voorstelbaar zijn. • De partij die de dienst of product levert uitgebreide toegang tot vertrouwelijke locaties, vertrouwelijke ICT-systemen en vitale infrastructurele installaties of werken, waarbij misbruik een nationaal veiligheidsrisico kan vormen. • Er zijn geen beheersmaatregelen mogelijk en realiseerbaar die de nationale veiligheidsrisico's – die in het geding – zijn voldoende beschermen. Het betreft hier onder andere landen die als zodanig zijn genoemd in de meest recente jaarverslagen en dreigingsbeelden van de MIVD en de AIVD. Een kleine groep landen die structureel wordt aangemerkt als de grootste statelijke cyberdreiging voor Nederland en vrijwel altijd worden genoemd zijn: Rusland, China, Iran en Noord-Korea.
---	---



4 NETWERKARCHITECTUUR & VERBINDINGEN

4.1 Begripsvorming

De netwerken verbinden (vrijwel) alle VGS en vormen zodoende een cruciaal aspect voor de goede werking van, en interactie tussen deze systemen. Onder **netwerk** wordt hier verstaan het geheel aan verbindingen ten behoeve van de communicatie tussen de componenten van VGS.

Qua type netwerken wordt onderscheid gemaakt tussen:

- **IP-netwerken**
 - Netwerken op basis van IP (Internet Protocol), zoals TCP en UDP. Deze netwerken zowel fysiek als logisch gescheiden worden, alsmede uit virtuele netwerken bestaan.
Diverse industriële protocollen kunnen ook over IP (BACnet/IP, Modbus TCP, KNXnet/IP, OPC UA, Ethernet/IP, etc.)
 - Voordeel: betrouwbare, beheersbare communicatie, veel securitymogelijkheden.
 - Risico: secure configuratie vereist expertise
- **IP-draadloze netwerken**
 - Draadloze communicatie kan op basis van IP (IPv4 of Ipv6: bijv. WiFi (IEEE 802.11), mobiele netwerken (4G, 5G), Zigbee IP, Thread, 6LoWPAN, BLE met IPSP, Wi-SUN), waaronder ook de meeste industriële protocollen over IP.
 - Voordeel: geen bekabeling, veel mogelijkheden tot secure configuratie.
 - Risico: eenvoudig te verstoren, kent veelal kwetsbaarheden, secure configuratie vereist expertise.
- **Niet-IP netwerken**
 - **Seriële netwerken**
 - 2, 3, 4 of meer-draads seriële communicatie (bijv. RS-232/485, veldbussen, industrieel Ethernet, CAN-bus)
 - Voordeel: goedkoop, eenvoudig en snel, geen aanvalsoppervlak malware en/of *lateral movement*.
 - Risico: afluister risico, geen cybersecuritymaatregelen behoudens fysieke afscherming.
 - **Contactbasis / signalering**
 - Analoge (continu variabel: °C omgezet naar 4–20mA, druk vertaald naar 0–10V, dimbare verlichting) of digitale (discreet: 0 of 1, 0V of 24V, open of dicht) harde i/o contacten. In dit geval is doorgaans enkel sprake van een koppelvlak en niet van een netwerk.
 - Voordeel: goedkoop, eenvoudig en snel, geen aanvalsoppervlak malware en/of *lateral movement*.
 - Risico: risico op manipulatie, geen cybersecuritymaatregelen behoudens fysieke afscherming.
- **Niet-IP draadloze netwerken**
 - Alle niet-IP gebaseerde draadloze communicatie, dat uiteenlopende protocollen kent (bijv. Zigbee, Z-Wave, Bluetooth, Lora, NFC, radiofrequenties).
 - Voordeel: geen bekabeling, veel mogelijkheden tot secure configuratie.
 - Risico: eenvoudig te verstoren, kent veelal kwetsbaarheden, secure configuratie vereist expertise.

Overall waar gesproken wordt over **netwerk** wordt 'IP-netwerk' en/of 'Draadloos IP-netwerk' bedoeld. Een **koppelvlak** is de afgesproken grens en wijze van interactie tussen twee systemen, componenten of zones, waarlangs communicatie, data, signalen, energie of fysieke objecten worden uitgewisseld.

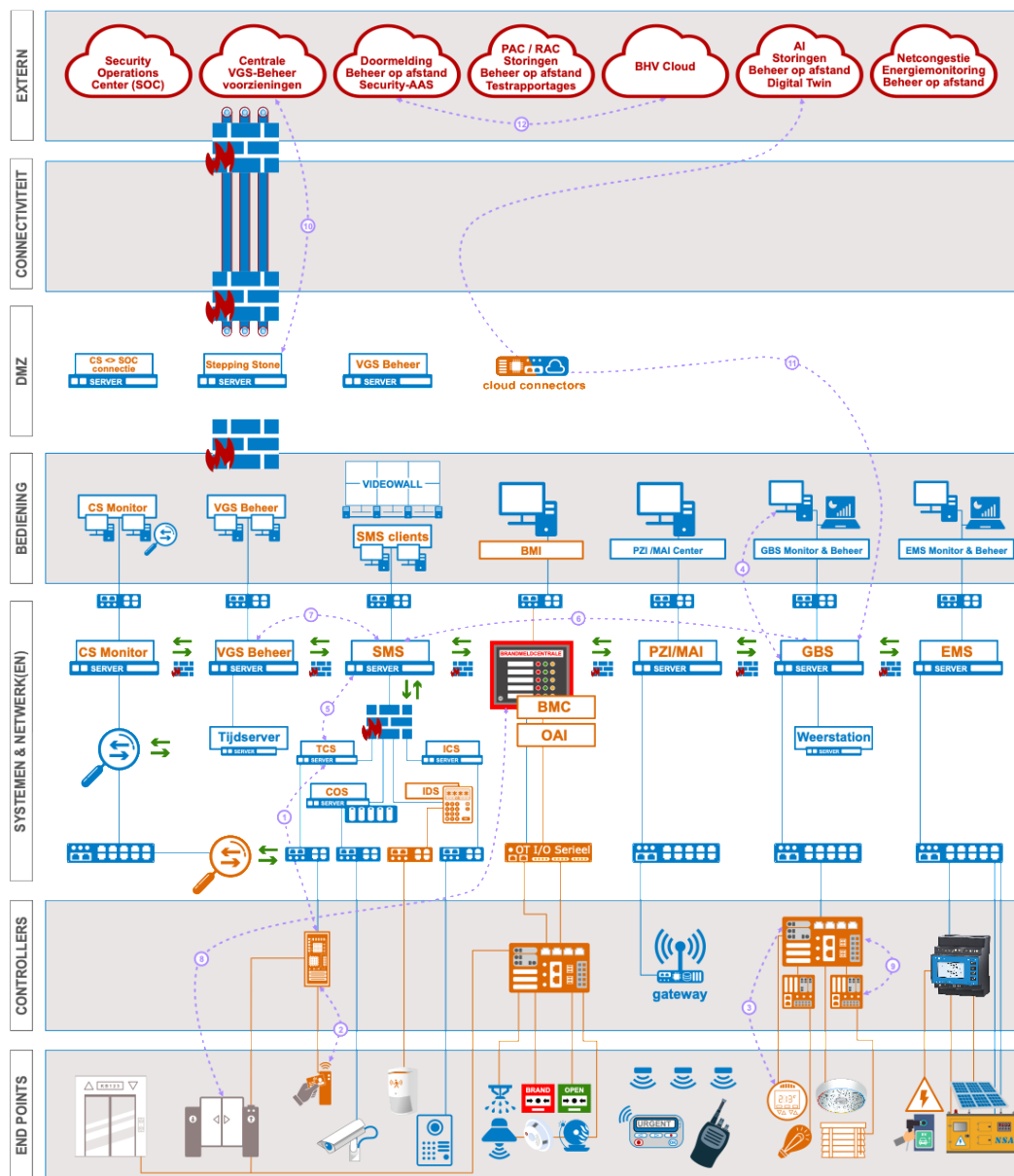
Communicatie over netwerken/koppelvlakken heeft meerdere verschijningsvormen:

- **Communicatie tussen de componenten** van het Vastgoed Gebonden Systeem.
 - Bijvoorbeeld: communicatie TCS server met controller (1), TCS controller met paslezer (2), controller met bedienpaneel (3), GBS server met bedienstation (4).
- **Communicatie tussen VGS** (of andere systemen) onderling op verschillende lagen.



- Bijvoorbeeld: communicatie tussen TCS en SMS server (5), tussen GBS en SMS server (6), tussen VGS-beheerserver en SMS (7), tussen BMI en vluchtdoor (8), tussen GBS controller en controller zonnewering (9).
- Communicatie van of naar externe bronnen, al dan niet met hun eigen netwerken.
 - Bijvoorbeeld: beheer op afstand (10), communicatie GBS met clouddienst (11), API's tussen clouddiensten (12).

Zie onderstaand voorbeeld ter illustratie.



4.2 Professioneel netwerk ontwerp en beheer

De netwerken verbinden (vrijwel) alle VGS en vormen zodoende een cruciaal aspect voor de goede werking van, en interactie tussen deze systemen. Hierom dient gedegen aandacht te worden besteed aan een professionele netwerkarchitectuur. Voor de netwerken is een blauwdruk vastgesteld.¹⁶ Hierbij gelden de volgende eisen.

¹⁶ Zie Verwijzing 06: VGS CS Architectuur documenten



O	E4.2-01	• Netwerken en externe verbindingen zijn professioneel ontworpen en gerealiseerd door vakbekwame specialisten (certificeringen als Cisco CCNA, Juniper JNCIA, Aruba ACSA of gelijkwaardig t.b.v. de realisatiefase).
O	E4.2-02	• De IP en draadloze netwerktopologie en bekabeling zijn conform de Digitale Vastgoedstandaard (DVS)¹⁷ en in lijn met het Handboek ICT-huisvesting en Bekabeling (HIB)¹⁸ of Kader Inrichting Eisen Netwerkruimtes (KIEN) in geval Defensie.
R	E4.2-03	• IP-netwerkcomponenten zijn afkomstig uit een enterprise-productlijn van één fabrikant en één productfamilie. De componenten zijn ontworpen voor professioneel, bedrijfskritisch gebruik en ondersteunen centraal beheer, configuratiebeheer, firmwarebeheer, monitoring, logging en detectie. Consumenten- en <i>small office, home office</i> (SOHO)-productlijnen zijn niet toegestaan. • Voor netwerken die omwille van certificering hierin niet in mee kunnen (bijv. brandmeldinstallatie) is dat vastgelegd.
O	E4.2-04	• Alle netwerken zijn inzichtelijk gemaakt in een <i>high-level design</i> en een <i>low-level netwerk design</i>, waarbij het onderscheid in type netwerken inzichtelijk is (zie voorbeeld in §4.1 Begripsvorming).
R	E4.2-05	• De Opdrachtnemer levert een centraal netwerkbeheer- en monitoringsysteem waarmee alle geleverde IP-netwerkcomponenten kunnen worden beheerd, bewaakt en geconfigureerd. Het beheersysteem ondersteunt ten minste: - Centrale monitoring van beschikbaarheid, prestaties, capaciteit en storingen van alle netwerkcomponenten. - Automatische detectie en rapportage van afwijkingen ten opzichte van de vastgestelde baselineconfiguratie. - Geprioriteerde alarmmeldingen met configureerbare ernstclassificaties en automatische doormelding van kritieke meldingen naar het centrale beheer- en/of securitymanagementsysteem. - Centraal configuratiebeheer inclusief versiebeheer, back-up, herstel en export van configuraties ten behoeve van audits, wijzigingsbeheer en incidentonderzoek. - Audit logging van beheeractiviteiten en ondersteuning van rolgebaseerde toegangsrechten.

¹⁷ RVB – Digitale vastgoed standaard (DVS), opvraagbaar

NB: De Digitale vastgoedstandaard biedt géén voorschriften m.b.t. beveiliging netwerkcomponenten en netwerkdiensten.

¹⁸ RVB - Handboek ICT-huisvesting en Bekabeling (HIB 3.0): <https://www.rijksvastgoedbedrijf.nl/documenten/2025/09/15/handboek-ict-huisvesting-en-bekabeling-hib-versie-3.0>



4.3 Netwerk Resilience

Resilience betreft de robuustheid van systemen en de weerbaarheid tegen (digitale) dreigingen, waaronder de mogelijkheid om zichzelf te herstellen of een zekere fouttolerantie te kunnen hebben.

O	E4.3-01	In geval van een complex (meerdere gebouwen) wordt redundantie in 2 <i>entrance facility</i> [EF] ruimtes geborgd die beide verbonden worden met 2 <i>campus distributor</i> [CD] ruimtes. Alle <i>building distributor</i> [DB] ruimtes worden vanuit beide CD-ruimtes gekoppeld als een dubbelster netwerk.
O	E4.3-02	In geval van een complex dient elk gebouw (bij verstoring van het campus netwerk) autonoom te blijven functioneren. Hiervoor dient het gebouw te beschikken over afdoende netwerkvoorzieningen en bedieningsmogelijkheden.
O	E4.3-03	In het geval van een gebouw (niet op een campus) wordt redundantie in 2 <i>entrance facility</i> [EF] ruimtes geborgd die beide verbonden worden met de 2 <i>building distributor</i> [BD] ruimtes, met uitzondering van Rijkskantoren kleiner dan 12.500 m² BVO¹⁹, indien hoge redundantie niet vereist wordt. In geval van Specialties is het uitgangspunt hoge redundantie, tenzij door Opdrachtgever anders is gespecificeerd in het contract.
O	E4.3-04	Core switches en/of centrale firewalls voor het netwerk hebben hoge beschikbaarheid en zijn redundant uitgevoerd als dubbelster netwerk naar <i>access switches in floor distributor</i> [FD] ruimtes of technische ruimtes, behoudens de situaties waarin expliciet geen hoge redundantie door Opdrachtgever wordt vereist.
O	E4.3-05	Alle <i>core</i>, distributie, server en storage switches alsmede firewalls (zijnde 'kritieke netwerkcomponenten') zijn voorzien van dubbele voedingen aan te sluiten op aparte groepen o.b.v. no-break (UPS) en noodstroom (NSA).
O	E4.3-06	In geval van meerdere tafels (werkstations beveiligers) in een meldkamer zijn de tafels verdeeld over verschillende elektra groepen, aangesloten achter <i>no-break</i> (UPS) en noodstroom (NSA) en gekoppeld op aparte switches, zodanig dat uitval van een groep of switch niet tot volledige uitval van de meldkamer leidt. Bij grotere meldkamers mogen maximaal 2 tafels achter dezelfde groep en switch.
O	E4.3-07	Endpoints voor beveiligingsapparatuur op access switches zijn in overleg met Opdrachtgever zodanig verdeeld over access switches dat bij uitval van één access switch de beveiliging niet blind is voor het aangesloten gebied en het primaire proces niet verstoord wordt. Enkel gebieden waar de beschikbaarheid laag of gemiddeld is, zijn hiervan uitgezonderd.
O	E4.3-08	Kritische componenten voor het betrouwbaar functioneren van het vastgoed gebonden systeem en single points of failure zijn inzichtelijk gemaakt.
O	E4.3-09	<i>Failover</i> van kritieke netwerkcomponenten en/of beperkte beschikbaarheid resulteert in een ondubbelzinnige, heldere en aanhoudende melding in het security management systeem (SMS) en/of andere daarvoor aangewezen managementsystemen. Dergelijke meldingen worden als security incident beschouwd en opgevolgd.

¹⁹ BVO: Bruto Vloeroppervlak



4.4 Netwerksegmentatie

Netwerksegmentatie is o.a. van belang om te voorkomen dat systemen elkaar onderling negatief kunnen beïnvloeden en (on)eigenlijke toegang tot een segment beperkt wordt.

O	E4.4-01	Netwerken van VGS dienen fysiek gescheiden te zijn van de netwerken voor de kantoorautomatisering van de Gebruiker en de netwerken voor de facilitaire organisatie. Netwerken van VGS hebben daarmee geén koppelvlakken zonder expliciete (schriftelijke) goedkeuring Opdrachtgever.
O	E4.4-02	- De volgende VGS-types beschikken over hun eigen, fysieke netwerk (switches, firewalls, glasvezels, koperbekabeling, ...) en mogen uitsluitend via firewalls en/of harde contacten gekoppeld worden: - Beveiligingssystemen (vanwege hogere classificatie) en specifiek voor het camerasysteem (vanwege bandbreedte). - Alle overige VGS
O	E4.4-03	Koppelingen tussen fysiek en tussen logisch gescheiden netwerken zijn middels next-gen firewalls beveiligd en geconfigureerd.
O	E4.4-04	- De volgende logische segmentatie wordt minimaal toegepast voor bijzondere systemen. Dat zijn systemen die - een kritische functie vervullen, - autonoom moeten functioneren, - in een andere beveiligingszone liggen en/of specifieke risico's kennen (dit laatste kan ook zijn met oog op beheer of verschillende betrokken partijen). Segmentatie VGS - Elk VGS vormt een apart segment - Elke locatie (gebouw) vormt een apart segment. - Aparte segmenten voor: - Servers - Clients - Management (beheer) voorzieningen - Cybersecurity/Performance monitoring - Niet toegewezen zone (voor alle nieuwe, nog toe te wijzen devices) dan wel quarantaine VLAN. - Aparte segmenten voor op IP-basis verbonden componenten die in meerdere zones voorkomen: - Buitengebied (bijv. parkeerterrein, toegangshek) - Publiek toegankelijke zones (bijv. receptie, wachtruimtes) - Beveiligde zone gebouw gedeeld met andere Gebruikers - Beveiligde zone gebouw voor medewerkers (t/m Dep.V) - Staatgeheim-confidentiële ruimte (Stg.C) - Staatgeheim-geheime ruimte (Stg.G) - Staatgeheim-zeer geheime ruimte (Stg.ZG)
O	E4.4-05	Systemen die een significant ander beveiligingsniveau en/of -configuratie hebben op basis van veiligheid, beschikbaarheid, integriteit en vertrouwelijkheid (bijv. als bestaande en nieuwe componenten toegepast worden), zijn logisch zodanig gescheiden dat ze onderling geen bedreiging kunnen vormen. Bijvoorbeeld: Camera's die NAC ondersteunen zijn logisch gescheiden van camera's die dat niet ondersteunen.



O	E4.4-06	Systemen met significant andere technologie of standaarden zijn logisch gescheiden. Bijvoorbeeld: Technologieën als informatietechnologie, operationele technologie en/of <i>Internet of Things</i> (IoT) horen van elkaar te zijn gescheiden.
O	E4.4-07	- Voor VGS-componenten die buiten staan, is het aanvalsoppervlak in ieder geval beperkt door toepassing van: - Sloten op kasten. - Anti-sabotagevoorzieningen. - Elektravoorzieningen naar object op aparte groepen met overspanningsbeveiliging. - Toepassing overspanningsbeveiliging voor dataverbindingen op basis van koper. - Uitsluitend glasvezelverbindingen (geen koper) voor dataverkeer tussen gebouw en objecten (bijv. fietsenstalling, parkeervoorziening) buiten de perimeter (hekwerk) van het terrein.
O	E4.4-08	Alle op IP-basis verbonden componenten in het buitengebied of publieke zones communiceren uitsluitend met de toegewezen server, gateway of controller en niet onderling (bijvoorbeeld d.m.v. <i>full port isolation</i>).
O	E4.4-09	Kwetsbare componenten zonder toereikende mitigerende maatregelen, zijn geïsoleerd.

4.5 Externe connectiviteit – Toepassing

Onder externe connectiviteit worden in dit kader alle verbindingen bedoeld die de gebouwgrenzen te buiten gaan. Externe verbindingen vergroten het aanvalsvlak, waardoor deze extra aandacht verdienen.

O	E4.5-01	Externe connectiviteit is <u>niet</u> toegestaan, tenzij als zodanig is gespecificeerd in Tabel 4.5-1: Toegestane externe connectiviteit ofwel expliciet, schriftelijk goedgekeurd door Opdrachtgever. Deze tabel wordt in het CSP overgenomen en aangevuld. In de tabel zijn reeds opgenomen uitzonderingen aangegeven met de volgende nummers: - Koppeling TCS met de Rijkspas, met tussenkomst van een next-gen firewall aan zijde beveiligingsnetwerk, die verkeer filtert en intrusie voorkomt. - Doormelding aan (particuliere) alarmcentrale van inbraakalarmen. In het geval van IP-verbinding met tussenkomst van een next-gen firewall. - Externe connectiviteit ten behoeve van optimalisatie klimaat, comfort en/of energieverbruik is toegestaan voor Rijkskantoren die als 'laag' risico geclassificeerd zijn. - Doormelding aan (particuliere) alarmcentrale van brandalarmen. In het geval van IP-verbinding met tussenkomst van een next-gen firewall.
O	E4.5-02	- Externe connectiviteit is toegestaan voor de toepassing van: - <i>Air gapped updates</i>. - Toepassing van een <i>scrubber</i>. - Koppelingen tussen locaties conform beleid en voorzieningen en netwerkinfrastructuur van de Gebruiker of Opdrachtgever. Op beide locaties dient het verkeer via een next-gen firewall te lopen met als doel dat locaties zich tegen elkaar kunnen beschermen t.a.v. digitale dreigingen en menselijke fouten. - Bij realisatie VGS-Architectuur of onderdelen daarvan door of onder regie van Opdrachtgever.

Er zijn verschillende situaties denkbaar inzake externe connectiviteit (kolommen tabel):



- A. **Uitgaande data:** data uit VGS wordt uit gebouw gestuurd. Bijvoorbeeld data voor energiemonitoring, storingsmeldingen, cybersecurity monitoring, etc.
- B. **Inkomende data:** data uit een externe bron dat ingelezen wordt in het VGS.
- C. **Kijkrechten** voor (storings)analyse: indien uitgaande data onvoldoende duiding geeft, zou urgentie en duiding nader bepaald kunnen worden met kijkrechten.
- D. **Bediening op afstand (door mens):** geeft beperkte rechten om parameters in VGS aan te passen (bijvoorbeeld setpoint voor temperatuur bij weerverandering).
- E. **Bediening op afstand (door machine):** geeft mogelijkheid om geautomatiseerd optimalisaties door te voeren op basis van algoritmes, externe informatie en/of AI.
- F. **Beheer op afstand** geeft ook mogelijkheid tot aanpassing van VGS op afstand.
- G. **Public clouddienst:** in een publieke clouddienst kunnen veel van bovenstaande opties gecombineerd worden.

De volgende tabel is door Opdrachtgever in overleg met Gebruiker (inzake *Specialties* ingevuld):

- ‘-’: type connectiviteit is **niet** toegestaan
- Nummer: toelichting op type connectiviteit en specifieke voorwaarden.

VGS Type	A	B	C	D	E	F	G
BEVEILIGING							
Security Management Systeem (SMS)	-	-	-	-	-	-	-
Toegangscontrolesysteem (TCS)	1	1	-	-	-	-	-
Cameraobservatiesysteem (COS)	-	-	-	-	-	-	-
Intercomsysteem (ICS) [verkeer, cel]	-	-	-	-	-	-	-
Inbraakdetectiesysteem (IDS)	2	-	-	-	-	-	-
Perimeterbeveiliging	-	-	-	-	-	-	-
E-sleutelkast	-	-	-	-	-	-	-
Vaste alarmknoppen	-	-	-	-	-	-	-
GEBOUWBEHEER							
Gebouwbeheersysteem (GBS)	3	3	3	3	3	3	3
Klimaatbeheersing (HVAC)	-	-	-	-	-	-	-
Zonwering	-	-	-	-	-	-	-
Aansturing verlichting	-	-	-	-	-	-	-
(I)IoT (multi)sensors	-	-	-	-	-	-	-
BRANDVEILIGHEID							
Brandmeldinstallatie (BMI)	4	-	-	-	-	-	-
Ontruimingsalarminstallatie (OAI)	-	-	-	-	-	-	-
Sprinklerinstallatie	-	-	-	-	-	-	-
Watermistinstallatie	-	-	-	-	-	-	-
Blusgasinstallatie	-	-	-	-	-	-	-
VEILIGHEID							
Personen Zoek Installatie (PZI)	-	-	-	-	-	-	-
Mobiele Alarm Installatie (MAI)	-	-	-	-	-	-	-
ELEKTRA							
(Nood) Verlichting	-	-	-	-	-	-	-
No break (UPS)	-	-	-	-	-	-	-
Noodstroom (NSA)	-	-	-	-	-	-	-
Energie monitoringsysteem	-	-	-	-	-	-	-
Zonnepanelen	-	-	-	-	-	-	-
Laadpalen	-	-	-	-	-	-	-
TRANSPORT							
Slagbomen	-	-	-	-	-	-	-
Bollards	-	-	-	-	-	-	-
Elektrische (draai)deuren	-	-	-	-	-	-	-
Speed lanes, sluisen	-	-	-	-	-	-	-
Roltrappen	-	-	-	-	-	-	-
Liften	-	-	-	-	-	-	-

Tabel 4.5-1: Toegestane externe connectiviteit



4.6 Externe Connectiviteit – Vereisten

Daar waar externe connectiviteit is toegestaan, zijn hier de eisen voor externe verbindingen (waaronder firewalls), een *demilitarized zone* (DMZ) en een stepping stone-server (jump server) benoemd waaraan voldaan moet worden.

O	E4.6-01	In geval van toepassing CSRA hebben MSP en SOC 24/7 toegang middels door de unit Weerbaarheid Geëvalueerde producten²⁰, bijvoorbeeld OpenVPN-NL. In dat geval voorziet MSP in de connectiviteitsbehoefte van leverancier die door het SOC gemonitord wordt. Indien van toepassing is een CSRA bouwblok hiervoor opvraagbaar.
O	E4.6-02	De VGS functioneren autonoom en hebben géén afhankelijk van externe connectiviteit om te functioneren.
O	E4.6-03	Inkomende mailservers zijn <u>niet</u> toegestaan in het netwerk van VGS (inkomende mail heeft <i>phishing</i> risico wat het aanvalsvlak vergroot).
O	E4.6-04	- Verschillende externe connecties zijn logisch van elkaar gescheiden. Het verkeer blijft in de DMZ gescheiden: - Voor connectiviteit naar verschillende locaties (bijvoorbeeld: een connectie met een cloud provider is gescheiden van connectie naar een leverancier voor beheer op afstand). - Voor verschillende richtingen van het verkeer (bijvoorbeeld: een uitsluitend uitgaande verbinding is gescheiden van een verbinding die zowel ingaand als uitgaand verkeer toestaat). - Voor data met een verschillende classificatie inzake vertrouwelijkheid (bijvoorbeeld: intern vertrouwelijke data is gescheiden van intern algemeen geclassificeerde data). - Voor verschillende typen VGS (bijvoorbeeld: data inzake beveiligingssystemen is gescheiden van data inzake gebouwbeheer).
O	E4.6-05	Externe verbindingen lopen altijd via een <i>dedicated</i> externe <i>next-gen firewall</i> (NGFW), die los staat van het interne VGS-netwerk. De <i>Demilitarized Zone</i> (DMZ) is vormgegeven in het gebied tussen de externe en interne firewall. De externe firewall is van een ander merk dan de interne firewalls i.v.m. potentiële kwetsbaarheden.
O	E4.6-06	Verkeer tussen firewall en externe bronnen is end-to-end versleuteld op basis van veilige encryptie die door het NCSC²¹ 'goed' bevonden is (momenteel TLS 1.3) (en bij onderdelen waar goed ontbreekt 'voldoende' is). In geval van als Departementaal Vertrouwelijk gerubriceerde VGS of data is versleuteling conform encryptie waarvoor de Unit Weerbaarheid een positief advies heeft gegeven, bijvoorbeeld OpenVPN-NL²⁰.
O	E4.6-07	- De externe firewall en DMZ-voorziening (server): - Zijn op basis van Security by Design & Default en zero-trust ingericht. - Firewall is default deny, alleen expliciet toegestane sessies mogen door. - Zijn real-time (geautomatiseerd) voorzien van de laatste updates voor <i>anti-malware</i>, <i>intrusion detection</i> en <i>prevention</i> (IDS/IPS) en <i>security patches</i>. - Zijn gehardend conform CIS level 2 of gelijkwaardig. Indien technisch of functioneel niet volledig haalbaar, worden afwijkingen onderbouwd en voorgelegd ter goedkeuring aan Opdrachtgever. Qua <i>hardening</i> is te allen tijde geborgd:

²⁰ Unit Weerbaarheid (Voorheen NBV: Nationaal Bureau Verbindingsbeveiliging) 'Geëvalueerde producten'.

²¹ <https://www.ncsc.nl/transport-layer-security> zie beveiligingsrichtlijnen



	▪ Firewall is niet extern en/of vanuit de DMZ te configureren, uitsluitend vanuit het interne netwerk voor de VGS. Firewall reageert extern niet op ping commando's e.d. ▪ Verwijdering van onnodige services en dichtzetten niet-noodzakelijke poorten. ▪ Standaard accounts en wachtwoorden verwijderen/deactiveren. - Worden periodiek (minimaal wekelijks) en op verzoek gescand op malware. - Logische toegang is gebaseerd op certificaten en multifactor authenticatie (MFA). <i>Bijvoorbeeld: 1: certificaat, 2: pin/wachtwoord/push, 3: posture of context check.</i> - Vóórdat verkeer naar interne services (DMZ of verder) mag wordt de identiteit gevalideerd (door bijvoorbeeld een Zero Trust Access Proxy (ZTNA) of reverse proxy achter de firewall): - Uitsluitend via <i>pull/get</i> mechanismen worden updates vanuit de <i>update server</i> aangevraagd worden bij de gecertificeerde, vertrouwde <i>online</i>-bronnen, die na downloaden gecontroleerd worden op integriteit. - De logbestanden van de firewall en apparatuur in de DMZ alsmede de detectiemiddelen (anti-malware, IDS, IDP) kunnen aangesloten worden op een SIEM/SOC. - Urgente alarmeringen inzake malware en/of intrusion worden direct gemeld en opgevolgd als security event. - In geval van een ernstige digitale dreiging dient deze omgeving direct, geautomatiseerd geïsoleerd te worden (losgekoppeld te worden van externe toegang en losgekoppeld van het netwerk voor VGS). - Toegang van administrator account conform <i>privileged user</i> uitgangspunten. - Firewall (extern en intern) configuraties dienen gedocumenteerd te worden, met per firewall-regel een beschrijving van het doel, en voorgelegd te worden aan Opdrachtgever voor accordering. Uitgangspunt dient te zijn dat altijd gebruikt wordt van de veilige, versleutelde variant van een protocol. Poorten die kwetsbaar zijn voor misbruik dienen in ieder geval altijd gesloten te zijn, bijvoorbeeld: SQL Server (1433), FTP (21), NetBIOS (139), RPC (593), Telnet (23), POP3 (110), IMAP (143), PPTP (1723) en SNMP (161), RDP (3389), SSH (22). - In geval van een <i>file transfer</i> optie dient deze afdoende beveiligd te zijn ingericht (FTPS, SFPT) en uitsluitend op basis van <i>whitelisting</i> vooraf vastgestelde IP locaties te functioneren.
O	E4.6-08 • Beheer op afstand verloopt altijd via een <i>stepping stone</i>, zodanig dat rechten en mogelijkheden goed beheersbaar blijven en nooit volledige of onbeheersbare noch oncontroleerbare toegang wordt versterkt.
O	E4.6-09 • Beheer op afstand vereist per sessie voorafgaand aan de sessie lokale vrijgave van de verbinding (bijv. door goedkeuring in lokaal systeem of verstrekking eenmalig te gebruiken wachtwoord of MFA code), op locatie is real time inzicht in alle actieve verbindingen, alle verbindingen worden gelogd en verbindingen hebben altijd een beperkt tijdsslot (standaard 2 uur, maximaal 8 uur per sessie) waarna de sessie verbroken wordt.



4.7 Inrichting Update proces

In deze paragraaf staan de eisen inzake de inrichting van het update proces.

Hierin worden 3 scenario's onderscheiden:

- **Scenario Gecontroleerd Verbonden:** Software en bestanden verlaten nooit de locatie en worden gecontroleerd ingebracht.
- **Scenario Air Gapped:** als scenario Isolatie maar additioneel *air gapped*
- **Scenario Vertrouwen en Verifiëren:** basis maatregelen set voor risicobewuste verificatie.

O	E4.7-01 Scenario Gecontroleerd Verbonden: in geval van renovaties, nieuwbouw en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...). • Software en bestanden verlaten nooit de locatie en worden gecontroleerd ingebracht. • Er is een centrale voorziening om updates online veilig op te halen uit gecertificeerde bronnen, dan wel bestanden aan te kunnen leveren. Dit vereist doorgaans: een externe verbinding, netwerkcomponenten, firewall, servercapaciteit in DMZ, scrubber/wasstraat, servercapaciteit in beveiligde zone die via interne firewall benaderd kan worden vanuit domein VGS. • In de beheerfase verrichten leveranciers werkzaamheden op de VGS middels speciaal daartoe voorziene en ingerichte beheerwerkplekken en/of beheerlaptops (die voldoen aan eisen zoals gesteld in CSR). En dus niet met eigen gegevensdragers en/of onderhoudslaptops. • Een wasstraat/scrubber proces controleert/verifieert gegevens die worden overgebracht naar het domein van VGS: - De wasstraat/scrubber controleert gegevens (updates, bestanden, ...) diepgaand op digitale dreigingen (o.a. d.m.v. meervoudige malware scans en controle op integriteit van updates/bestanden). - De wasstraat/scrubber controleert gegevens die op fysieke gegevensdragers worden aangeleverd. Zie voor beeldvorming 0 Bijlage D : Voorbeeld ontwerp toepassing scrubber.
O	E4.7-02 Scenario Air Gapped: in geval van een locatie met hogere rubricering (Staatsgeheim) of op locaties waar externe connectiviteit met het systeem niet is toegestaan: • Er is een centrale voorziening om updates online veilig op te halen uit gecertificeerde bronnen, dan wel bestanden aan te kunnen leveren (zie E4.7-01). Deze voorziening is losgekoppeld van het domein VGS, zijnde <i>air gapped</i>. • Gegevens die worden overgebracht naar het domein van VGS worden gecontroleerd/geverifieerd middels het wasstraat/scrubber proces (zie E4.7-01). - De gegevens worden na controle overgezet op een daartoe aangewezen gegevensdrager. - De gegevens worden versleuteld en voorzien van certificaat (of vergelijkbaar). - In het domein van VGS kan de door de wasstraat/scrubber gecontroleerde data (vanwege versleuteling en certificaat) uitsluitend worden ingelezen op een daartoe aangewezen locatie (server). - Voor een Vastgoed Gebonden Systeem dat als Staatsgeheim is gerubriceerd, is de aangewezen locatie (server) gescheiden van de VGS door een datadiode. Dit om te borgen dat gegevens het Staatsgeheim netwerk niet kunnen verlaten. Zie voor beeldvorming 0 Bijlage D : Voorbeeld ontwerp toepassing scrubber.



B	E4.7-03 Scenario Vertrouwen en Verifiëren: in geval van ‘laag risico’ locaties en VGS dat niet hoger is gerubriceerd dan Departement Vertrouwelijk en voor minder omvangrijke projecten dan benoemd in E4.7-01. Dit scenario kan ook selectief voor een VGS worden toegepast, indien aangetoond is dat een beheerlaptop op locatie niet haalbaar is. In dit geval dienen de betrokken onderhoudspartijen bewust te zijn van de risico's en dienen zij aan te tonen dat voor hun apparatuur (bijvoorbeeld beheerlaptops) volgende maatregelen zijn genomen conform beleid (<i>hardening</i>, voorzien van wachtwoord, versleutelde harddisk, host-firewall, malware scanner met actuele handtekeningbestanden, geen mogelijkheid software te installeren, <i>remote lock/wipe</i>, etc.). Voorafgaand aan het moment dat de apparatuur gekoppeld wordt, dient geverifieerd te worden dat in ieder geval, volgendeljk: • Software updates/patches/handtekeningbestanden vanuit geverifieerde bronnen (o.b.v. certificaten en/of <i>hashes</i>) van het besturingssysteem en de anti-malware software zijn doorgevoerd. • Eventuele updates/configuraties voor het Vastgoed Gebonden Systeem zijn gedownload vanuit vertrouwde en geverifieerde bronnen (o.b.v. certificaten en/of <i>hashes</i>). • Eventuele passieve media (USB-stick, CD-Rom, etc.) dienen altijd vooraf op malware te worden gescand vanuit vertrouwde beheerapparatuur. • Smartphones en/of tablets mogen <u>niet</u> worden ingezet voor beheerwerkzaamheden. • Er een anti-malware scan wordt uitgevoerd (met actuele handtekeningbestanden) minimaal op interne geheugen, kritische gebieden en de toe te passen updates/bestanden. • Externe connecties (WiFi, 4G, Bluetooth, etc.) zijn uitgeschakeld.
---	--

4.8 Draadloze technologie – registratie en goedkeuring

Draadloze technologie kan het aanvalsoppervlak vergroten en kan een bereik hebben buiten de zone waarvoor het bedoeld is, waardoor hier extra aandacht voor moet zijn.

O	E4.8-01 • Draadloze communicatietechnologieën zijn niet toegestaan, tenzij expliciet kenbaar gemaakt en door Opdrachtgever schriftelijk goedgekeurd (bijvoorbeeld vanwege beveiliging, interferentie, gezondheid, etc.).
O	E4.8-02 • Draadloze NFC technologie voor paslezers is toegestaan, voor specificatie en vereisten wordt verwezen naar de beveiligingsvereisten voor toegangscontrole. Af te stemmen met de Adviseur Beveiliging van het Rijksvastgoedbedrijf en gebaseerd op de meeste actuele versie van het Normenkader Beveiliging Rijkskantoren (NkBR) en/of Normenkader Rijkspas (beide documenten zijn niet openbaar beschikbaar).
O	E4.8-03 • Alle Draadloze communicatie wordt behandeld als Externe connectiviteit.



4.9 Netwerktogang & authenticatie

Het is van belang dat er te allen tijde een compleet beeld is van de op het netwerk aangesloten *devices*. Network Access Control (NAC, 802.1x) is een methode om *devices* op basis van certificaten te authenticeren. Oude methoden als port security (o.b.v. MAC adres) hebben een veel lager niveau van beveiliging, hetgeen onderdeel moet zijn in de risicoafweging.

O	E4.9-01	Op het netwerk van VGS mogen alleen <i>devices</i> aangesloten worden die onderdeel vormen van, of directe relatie hebben met de functionaliteit van de VGS. Indien <i>rogue devices</i> (componenten die geen onderdeel zijn van de VGS) aangesloten worden, wordt dit directesignaleerd en opgevolgd.
O	E4.9-02	- Het streven is alle <i>devices</i> van VGS met Network Access Control (NAC, 802.1x) op het netwerk te authenticeren. Toepassing van Network Access Control (NAC, 802.1x) geldt als <u>minimale eis</u> bij onderstaande IP <i>devices</i>: - IP-componenten in buitengebied en publieke zone die zichtbaar zijn (dus niet indien ze in een met slot afgesloten kast zitten die onder detectie staat). - Client PC's, bedien PC's, beheer PC's/laptops, jump servers - Camera's - Intercoms - Bedienpanelen (bijv. t.b.v. temperatuur, verlichting, zonnewering) - Smart devices (bijv. IoT multisensors) - Controllers / PLC in geval van classificatie als hoog of kritiek. Denk hierbij aan deurcontrollers voor toegangscontrole, GBS controllers voor gebouwautomatisering, etc. - Systemen en/of devices waarbij NAC technisch mogelijk is bij 3 of meer gangbare, marktconforme leveranciers die dit adviseren in hun security advies.
O	E4.9-03	- Daar waar de VGS-veldapparatuur niet geschikt is voor NAC: - Is dat ondubbelzinnig inzichtelijk gemaakt in het CSP. - Is dat onderbouwd en wordt jaarlijks geëvalueerd (alsnog te realiseren?). - MAB (<i>MAC Authentication Bypass</i>) is toegepast met <i>whitelisting</i>, dynamisch VLAN toewijzing en onbekende MAC-adressen naar quarantaine VLAN en gebruik access control list (ACL). <i>Port security</i> is toegepast op basis van minimaal aantal benodigde MAC-adressen voor de betreffende poort - Ondubbelzinnige alarmering bij overtredingen (<i>violations</i>).
R	E4.9-04	Certificaten t.b.v. NAC: - Opdrachtnemer draagt zorgt voor de certificaten, beheert ze en stelt deze beschikbaar aan Opdrachtgever. - Indien technisch mogelijk worden certificaten via een geautomatiseerd proces of script vervangen. De geldigheidstermijn van certificaten wordt nader afgestemd te worden met Opdrachtgever in relatie tot de beheerafspraken. Als uitgangspunt geldt een oneindige geldigheid, welke kan worden verkort indien goed geborgd in beheerafspraken: - Handmatig vervangen: minimaal elke 5 jaar. - Geautomatiseerd te vervangen: minimaal elke 1,5 jaar. - afhankelijk ontwerp, goedkeuring OG. Bepalen in Definitiefase door OG. - Er dient minimaal 10% van het aantal certificaten extra beschikbaar te worden gesteld voor de beheerorganisatie met oog op onvoorziene wisselingen en uitbreiding van de apparatuur.



	• De privé-sleutels mogen onder geen enkel beding kenbaar worden gemaakt en bij implementatie mag het op geen enkele manier mogelijk zijn om kennis te nemen van de sleutel. • De geldigheid van certificaten wordt in rapportages ondubbelzinnig inzichtelijk gemaakt en er wordt gealarmeerd indien geldigheid van certificaten korter is dan 3 maanden. • De uitgegeven certificaten zijn eigendom van Opdrachtgever en worden overgedragen aan Opdrachtgever. Opdrachtgever kan beheer hiervan eventueel overdragen aan een aangewezen vertrouwde leverancier voor onderhoud. • Opdrachtgever behoudt zich het recht voor om de frequentie van certificaatvervanging te herzien en/of certificaten zelf, dan wel via derden, beschikbaar te stellen, welke door Opdrachtnemer worden toegepast.
--	--

4.10 Versleuteling communicatie – data in transit

Versleuteling van communicatie (data in transit) zorgt dat de vertrouwelijkheid geborgd wordt alsmede de integriteit.

O	E4.10-01	• Alle communicatie (data in transit) is ‘verantwoord versleuteld’. Dit geldt als <u>minimale eis</u> voor: - Communicatie die onderdeel is van logische toegang (bijvoorbeeld: inloggegevens, wachtwoorden, certificaten, MFA-tokens). - Communicatie van vertrouwelijke gegevens (Intern Vertrouwelijk of hoger). - Communicatie van persoonsgegevens (bijvoorbeeld: toegangscontrole, cameratoezicht, gespreksopname, biometrie, smart building). - Communicatie met een classificatie integriteit hoog of kritiek. - Systemen waarbij versleuteling van data in transit dit technisch mogelijk is bij 3 of meer gangbare, marktconforme leveranciers. • Onder ‘verantwoord versleuteld’ wordt verstaan: - Toepassing van niet-kwetsbaar bevonden encryptie, passend op risicoduiding en functioneel haalbaar met oog op vereiste prestaties van het VGS. - Versleuteling op basis van TLS met veiligheidsniveau ‘goed’ conform NCSC²². - Indien veiligheidsniveau ‘goed’ technisch niet haalbaar is mogen TLS-opties met veiligheidsniveau ‘voldoende’ in nieuwe projecten toegepast worden, zij het uitsluitend met goedkeuring Opdrachtnemer, na onderbouwing.
O	E4.10-02	• Alternatieve versleuteling tussen apparaten en/of tussen netwerken als bijvoorbeeld <i>site-to-site</i> VPN, SSH, SRTP, SIPS, <i>lightweight cryptography</i> (LWC) is, mits veilig bevonden, toegestaan na toetsing en schriftelijke goedkeuring van Opdrachtgever.
B	E4.10-03	• De toegepaste TLS-versies en/of andere versleuteling worden jaarlijks getoetst aan de hand van de meest recente publicatie van het NCSC of andere gerenommeerde bronnen. Voor TLS-versies met veiligheidsniveau ‘voldoende’, wordt vervanging nagestreefd. TLS-versies met veiligheidsniveau ‘uit te faseren’, worden binnen 6 maanden vervangen.

²² <https://www.ncsc.nl/documenten/publicaties/2025/juni/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05>



4.11 Veilige protocollen

Protocollen kunnen kwetsbaar zijn of zelfs standaard onversleuteld zijn. Daar waar veilige alternatieven zijn, zijn deze toegepast

A	E4.11-01	Er is gekozen voor veilige, niet-kwetsbare protocollen (<i>security by design</i>) die op de juiste manier (<i>security by default</i>) geconfigureerd zijn.
R	E4.11-02	Niet versleutelde verbindingen zijn ondubbelzinnig inzichtelijk gemaakt middels de eisen in H6 KOPPELVLAKKEN TUSSEN SYSTEMEN.

Voorbeelden (niet limitatief) van onveilige protocollen en mogelijke alternatieven zijn:

ONDERWERP	ONVEILIG	MOGELIJK ALTERNATIEF
Bestandsoverdracht	FTP, TFTP	SFTP (SSH), FTPS (TLS), SCP
Communicatie	OPC BACnet SNMP v1, 2	OPC-UA BACnet Secure Connect (B/SC) SNMP v3
Communicatie active directory	LDAP (poort 389)	LDAPS/Secure LDAP (poort 636) Kerberos
Communicatie toegangscontrole	Wiegand	OSDP (Open Supervised Device Protocol), RS-485-gebaseerde protocollen met encryptie, TLS
Encryptie	Symmetrisch: DES, 2DES, Blowfish, RC2, RC5 Asymmetrisch: RC4 Real-time Transport Protocol (RTP)	Symmetrisch: AES Asymmetrisch: RSA Secure RTP (SRTP)
Hashes	MD5, SHA-1	SHA2 (≥ 256), SHA-3, RIPEMD (≥ 256), zie ook de NCSC beveiligingsrichtlijnen ²³
Hyper text	HTTP	HTTPS
Radius	TACACS, XTACACS	TACACS+ of RADIUS
Tijdsynchronisatie	NTP	Secure NTP of Network Time Security (NTS)
TLS	SSL, TLS 1.1	TLS 1.3 of hoger
Toegang op afstand	Telnet	SSH

²³ NCSC beveiligingsrichtlijnen zie <https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1>



5 VASTGOED GEBONDEN SYSTEMEN

In dit hoofdstuk wordt specifiek ingegaan op de componenten (hard- en softwarematig) waaruit de VGS zijn opgebouwd. Dit hoofdstuk bevat een selectief aantal aspecten

Uiteindelijk gaat het om de functionaliteit van de VGS en de onderlinge communicatie tussen deze systemen. Steeds meer van deze systemen maken gebruik van 'IT-componenten' als Windows/Linux besturingssystemen, SQL-databases, IT-communicatieprotocollen, etc. Aan de andere kant zien we nog de nodige industriële toepassingen en protocollen.

5.1 Betrouwbaar & Robuust

R	E5.1-01	Voor de realisatie is betrouwbare, robuuste en bewezen hard- en software toegepast die voldoet aan de benodigde veiligheids- en beveiligingseisen en geschikt is voor de specifieke omgeving waarin het toegepast is.
R	E5.1-02	Er mogen geen componenten ingezet worden met achterdeurtjes, zijnde: componenten die kunnen communiceren op een wijze waarbij de normale beveiligingsmaatregelen worden omzeild.

5.2 Hardening

R	E5.2-01	- Alle netwerk-, ICT-componenten, besturingssystemen en/of applicaties waarvoor een CIS²⁴ hardening benchmark bestaat zijn - Conform de eisen van CIS level 1 gehardend. - In geval van kritisch geclassificeerde VGS op CIS level 2 gehardend. Daar waar technisch en/of functioneel dit niet volledig haalbaar is, zijn afwijkingen onderbouwd en voorgelegd ter goedkeuring aan Opdrachtgever.
R	E5.2-02	Beleid (<i>policies</i>) worden centraal beheerd. Denk aan group policies (GPO) in Microsoft Windows producten, <i>Mobile Device Management</i> (MDM) in iOS/Android producten (ook bijvoorbeeld tablets voor bediening) of specifieke tools voor Linux. Daar waar dit niet mogelijk is, is dit onderbouwd en voorgelegd ter goedkeuring aan Opdrachtgever.
R	E5.2-03	- Indien voor een VGS-component geen toepasselijke CIS Benchmark beschikbaar is, wordt de component aantoonbaar gehardend conform de beveiligingsrichtlijnen van de fabrikant en algemeen geaccepteerde security best practices. De hardening omvat ten minste de volgende maatregelen: - Alle niet-functioneel noodzakelijke services, software, applicaties, kernelmodules en besturingssysteemcomponenten zijn verwijderd of uitgeschakeld. Waar technisch mogelijk wordt applicatie-whitelisting toegepast. - De host-firewall is geconfigureerd volgens het default deny-principe. Beheer op afstand is uitsluitend toegestaan via geautoriseerde beheerprotocollen, vanaf geautoriseerde beheersystemen en voor het functioneel noodzakelijke netwerkverkeer. - Besturingssysteem- en platformconfiguraties zijn ingesteld conform actuele beveiligingsrichtlijnen en best practices. - Fysieke interfaces voor gegevensoverdracht, zoals USB-poorten en SD-kaartlezers, zijn standaard uitgeschakeld. Indien gebruik functioneel noodzakelijk is, is dit

²⁴ CIS benchmarks: <https://www.cisecurity.org/cis-benchmarks>



		aantoonbaar onderbouwd, expliciet geautoriseerd en zijn passende mitigerende maatregelen getroffen. - BIOS-, UEFI- en vergelijkbare firmware-instellingen zijn beveiligd met unieke, complexe beheerderswachtwoorden of een gelijkwaardig authenticatiemechanisme en ongeautoriseerde wijzigingen zijn niet mogelijk.
R	ES.2-04	• Er is geen directe verbinding met het internet, zodat het direct downloaden van bestanden/software en/of browsen op internet niet mogelijk is.
R	ES.2-05	• Individuele gebruikers kunnen op hun werkomgeving (die onderdeel uitmaakt van de VGS) zelf niets installeren, anders dan via de verantwoordelijke ICT-beheerder wordt aangeboden of wordt toegestaan (<i>whitelist</i>).
R	ES.2-06	• Daar waar kioskmodus is toegepast, is deze dusdanig ingericht dat er redelijkerwijs niet is uit te breken.
R	ES.2-07	• Alleen vanuit beheerstations (dus nooit vanuit werkplekken individuele gebruikers) is het mogelijk servers te benaderen met <i>privileged accounts</i> om beheertaken te kunnen uitvoeren.

5.3 VGS Resilience

Resilience betreft de robuustheid van systemen en de weerbaarheid tegen (digitale) dreigingen, waaronder de mogelijkheid om zichzelf te herstellen of een zekere fouttolerantie te kunnen hebben.

O	ES.3-01	In het geval van toepassing van de CSRA geldt dat: - Dat beheervoorzieningen die de VGS direct kunnen beïnvloeden, redundant en hoog beschikbaar worden uitgevoerd. (bijvoorbeeld: bij uitval Active Directory kan je niet inloggen op VGS dat daarop gekoppeld is) - Dat VGS dat virtueel uitgevoerd wordt op de server infrastructuur, redundant wordt uitgevoerd. In geval dit technisch of anderszins niet haalbaar is, vereist dit expliciete goedkeuring van de Opdrachtgever. Uitzondering hierop is als het VGS als laag is geclassificeerd qua beschikbaarheid. - De server infrastructuur zelf dient te worden opgebouwd o.b.v. beschikbaarheidsclassificatie kritiek.
O	ES.3-02	• In geval van een complex (meerdere gebouwen) dient elk gebouw autonoom te kunnen functioneren. Hiervoor dient het gebouw te beschikken over afdoende servercapaciteit en bedieningsmogelijkheden.
O	ES.3-03	• Kritiek en hoog risico VGS qua beschikbaarheid zijn in hoge-beschikbaarheid uitgevoerd en zijn redundant uitgevoerd in gescheiden, daarvoor geschikte ICT-ruimtes en schakelen in geval van uitval/verstoring direct (binnen maximaal 1 minuut) over (<i>failover</i>).
O	ES.3-04	• Alle servers zijn voorzien van dubbele voedingen aan te sluiten op aparte groepen o.b.v. <i>no-break</i> (UPS) en noodstroom (NSA).
O	ES.3-05	• Alle servers voor Kritiek en hoog VGS qua beschikbaarheid zijn voorzien van dubbele netwerkaansluitingen en zijn aangesloten op aparte server switches.
O	ES.3-06	• Virtualisatie van meerdere vastgoed gebonden systemen op eenzelfde server is toegestaan, indien: - Alle vastgoed gebonden systemen een failover hebben op een 2^{de} redundante server en beide servers gemonitord worden door een witness server. - Virtualisatie van het vastgoed gebonden systeem ondersteund wordt door de fabrikant.



		- De vastgoed gebonden systemen elkaar niet verstoren in hun werking. - De type VGS 'Beveiliging' fysiek gescheiden zijn van andere type vastgoed gebonden systemen. Binnen type VGS Beveiliging dient het Cameraobservatiesysteem over een eigen, dedicated server(s) te beschikken. - Er geen wezenlijke aandachtspunten voortkomen uit verschillen in rubricering.
O	ES.3-07	• Kritische componenten voor het betrouwbaar functioneren van het vastgoed gebonden systeem en single points of failure zijn inzichtelijk gemaakt.
R	ES.3-08	• Opslagvoorzieningen bieden minimaal de volgende fouttolerantie: - Voor VGS met een gemiddelde beschikbaarheidseis wordt minimaal een RAID-niveau toegepast dat bestand is tegen het uitvallen van één opslagmedium (bijvoorbeeld RAID 5 of ZFS RAIDZ1). - Voor VGS met een hoge of kritieke beschikbaarheidseis wordt minimaal een RAID-niveau toegepast dat bestand is tegen het gelijktijdig uitvallen van twee opslagmedia (bijvoorbeeld RAID 6 of ZFS RAIDZ2). - Bij gedeelde opslagplatformen of storageclusters wordt minimaal een configuratie toegepast die meerdere redundante RAID-sets combineert (bijvoorbeeld RAID 60 of ZFS RAIDZ3), of een aantoonbaar gelijkwaardig beschermingsniveau biedt. - RAID-groepen worden zodanig gedimensioneerd dat de kans op dataverlies tijdens een rebuild aantoonbaar wordt beperkt. Hierbij worden de aanbevelingen van de fabrikant gevolgd ten aanzien van het maximale aantal opslagmedia per RAID-groep. Indien een andere opslagtechniek dan RAID wordt toegepast (zoals erasure coding, replicatie of een software-defined storage-oplossing), dient deze aantoonbaar een gelijkwaardig of hoger niveau van beschikbaarheid en gegevensbescherming te bieden.
R	ES.3-09	• <i>Failover</i> van een server en/of beperkte beschikbaarheid resulteert in een ondubbelzinnige, heldere en aanhoudende melding in het security management systeem (SMS) en/of andere daarvoor aangewezen management systemen. Dergelijke meldingen worden als security incident beschouwd en opgevolgd.
R	ES.3-10	• Alle Windows en Linux machines binnen een object worden uitgerold met de meest actuele Long-Term Servicing Channel (LTSC)-versies.
B	ES.3-11	• Van VGS die als kritisch zijn geclassificeerd, zijn componenten die bij uitval het functioneren van het systeem wezenlijk kunnen verstoren (>20%) binnen 8 uur leverbaar of op voorraad.

5.4 Versleuteling – data at rest

O	ES.4-01	• Alle opgeslagen data (<i>data at rest</i>) is afdoende versleuteld, Dit geldt als <u>minimale eis</u> voor: - Gegevens die onderdeel uitmaken van logische toegang (bijvoorbeeld: inloggegevens, wachtwoorden, certificaten, MFA tokens). - Vertrouwelijke gegevens (Intern Vertrouwelijk of hoger). - Persoonsgegevens (bijvoorbeeld: toegangscontrole, cameratoezicht, gespreksopname, biometrie, smart building). - Gegevens van een VGS, koppelvlak en/of datastroom met Integriteitsclassificatie hoog of kritiek. • Deze voorwaarde is alleen van toepassing indien technisch mogelijk bij 3 of meer gangbare, marktconforme leveranciers.
R	ES.4-02	• Verantwoorde versleuteling:



	- Toepassing van niet-kwetsbaar bevonden encryptie, passend op risicoduiding en functioneel haalbaar met oog op vereiste prestaties van het VGS.
--	--

5.5 Mobiele apparatuur

Mobiele apparatuur kan het aanvalsoppervlak vergroten, waardoor hier extra aandacht voor moet zijn.

Mobiele apparatuur als mobiele telefoons, porto's, pagers, tablets, mobiele alarmknoppen, afstandsbedieningen, etc. kunnen al dan niet een directe relatie hebben met de VGS.

O	ES.5-01	• In geval van renovaties, nieuwbouw en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...) en in geval van een locatie met hogere rubricering (Staatsgeheim) wordt bij onderhouds- en beheerwerkzaamheden uitsluitend gewerkt met een beheerlaptop die op locatie blijft. Indien dit niet haalbaar is, wordt dit onderbouwd en voor expliciete goedkeuring aan Opdrachtgever voorgelegd.
R	ES.5-02	• Mobiele apparatuur wordt uitsluitend ingezet na voorafgaande schriftelijke goedkeuring van de Opdrachtgever, waarbij vervangende apparatuur minimaal aan hetzelfde beveiligingsniveau voldoet en opnieuw expliciet is goedgekeurd.
R	ES.5-03	• Bij de inzet van mobiele apparatuur van VGS t.b.v. gebruik en/of beheer zijn minimaal de volgende aspecten geïmplementeerd: - Er zijn duidelijke instructies over het veilig en verantwoord gebruik van mobiele <i>devices</i> opgesteld en gecommuniceerd (als onderdeel training & bewustwording). - Er is aantoonbaar procesmatige borging van patchmanagement en <i>hardening</i> van de <i>devices</i>, ze zijn professioneel beveiligd en data op het <i>device</i> is versleuteld. - De <i>devices</i> worden centraal beheerd middels een professionele oplossing (bijv. <i>Mobile Device Management</i> - MDM), zodat beleid op de <i>devices</i> afgedwongen wordt, vermiste <i>devices</i> gelokaliseerd worden die op afstand geblokkeerd en gewist kunnen worden. - Oneigenlijke (<i>rogue</i>) <i>devices</i> kunnen geen toegang tot het netwerk verkrijgen.
B	ES.5-04	• Indien mobiele apparatuur in bruikleen wordt gegeven tekenen individuele gebruikers een overeenkomst voor mobiel werken, waarmee zij verklaren zich bewust te zijn van de gevaren van mobiel werken en verklaren dit veilig te zullen doen.

5.6 Specifiek

Laadpalen

A	ES.6-01	• Voor laadpalen die als directielevering vanuit een centrale overeenkomst van het RVB worden geleverd, geldt dat die partij de verantwoordelijkheid draagt voor de cybersecurity van de laadpalen en dienstverlening.
O	ES.6-02	• M.b.t. de laadpalen (voor medewerkers, bezoekers) vanuit het project gelden de <i>Security requirements for procuring EV charging stations</i>²⁵ van het European Network for Cyber Security (ENCS), met minimalisatie van het aantal connecties/partijen.
O	ES.6-03	• Laadpalen (voor medewerkers, bezoekers) die zijn aangesloten op de elektra voorzieningen van het gebouw dienen via energiemeters gemonitord te worden, waarbij nóóit sprake is van een IP-verbinding met enig VGS.
O	ES.6-04	• Voor laadpalen die het primaire proces ondersteunen (voor bijvoorbeeld dienstvoertuigen) geldt aanvullend dat externe (cloud)diensten niet zijn toegestaan.

²⁵ 'EV-311: <https://encs.eu/resource/ev-311-security-requirements-from-iec-62443-for-procuring-ev-charging-stations/>



	Uitgangspunt is dat laadstations zijn aangesloten op een energiemonitoring- of power managent systeem.
--	--



6 KOPPELVLAKKEN TUSSEN SYSTEMEN

Inzicht in alle koppelvlakken is van belang. Een koppelvlak tussen systemen is een interessant aanvalspunt omdat het vaak configuraties bevat van de gekoppelde systemen en een verbinding tussen de systemen biedt. Voor het inzichtelijk maken moet een blauwdruk van de koppelvlakken zijn aangeleverd.

O	E6.1-01	Alle koppelvlakken tussen vastgoed gebonden systemen – inclusief koppelvlakken met systemen die in het kader van de opdracht out-of-scope zijn – zijn inzichtelijk gemaakt.
O	E6.1-02	Koppelvlakken zijn met beveiligde protocollen te vormgeven, waarbij de data-overdracht (<i>data in transit</i>) versleuteld is conform de eisen in §4.10 Versleuteling communicatie – data in transit.
O	E6.1-03	Koppelvlakken zijn zodanig ontworpen en geconfigureerd dat het onnodig distribueren van vertrouwelijke data of persoonsgegevens wordt voorkomen.
O	E6.1-04	- De koppelvlakken tussen logisch of fysiek gescheiden netwerken zijn expliciet onderbouwd qua ontwerp en beveiliging op alle lagen. Hiertoe is gespecificeerd: - <u>Doel</u>: wat is het doel van de koppeling, waarvoor dient deze? - <u>Bron- en doelsysteem</u>: tussen welke systemen wordt gekoppeld? - <u>Welke data</u> wordt gecommuniceerd in welke richting? - <u>Zones</u>: Hoe zijn de verschillende systemen (zones) geclassificeerd? ▪ Vertrouwd: • zelfde type systeem (bijv. beveiliging, gebouwbeheer, ...), • zelfde beveiligingsniveau zone, • zelfde beheerpartijen. ▪ Semi-vertrouwd: • Zelfde type systeem, maar ander beveiligingsniveau zone en/of andere beheerpartijen (bijv. SMS versus sleutelkast of GBS versus koelmachine). • Verbindingen met andere locaties/gebouwen op complex of met satellietlocaties binnen directe invloedssfeer van Opdrachtgever of Gebruiker. ▪ Laag-vertrouwd: • Ander type systeem (bijv. koppeling tussen beveiliging en gebouwbeheer), maar wel binnen VGS scope Opdrachtgever. ▪ Niet-vertrouwd • Niet-vertrouwd-Intern: koppelingen met systemen buiten VGS scope Opdrachtgever binnen de locatie. • Niet-vertrouwd-Extern: koppelingen buiten de locatie via internet, satelliet, ... - <u>Barrier</u>: via welke apparatuur de koppeling verloopt. Bijv. rechtstreeks, via switches, converter, firewall, <i>data diode</i>, filterende router of gateway. - <u>Kenmerken koppeling</u>: digitaal (TCP/IP) over koper(S/FTP)/glas, API/SDK, 2 of 4-draads serieel (bijv. RS-232, RS-485), draadloos, contactbasis (analoge of digitale harde i/o contacten). - <u>Protocollen</u>: volgens welke protocollen (bijv. Secure LDAP via TCP/IP, of Modbus RTU via RS-485, BACnet over Zigbee). - <u>Versleuteling</u>: specificatie van versleuteling. - <u>Verantwoordelijkheid</u>: de verantwoordelijke voor het koppelvlak. - <u>Betrouwbaarheid</u>: toegepaste verificatie/validatie om ▪ de betrouwbaarheid van gegevensoverdracht te borgen en



	▪ verkeerde pakketten te detecteren ▪ te voorkomen dat verkeerde pakketten schade veroorzaken.
--	--



7 SECURITY MONITORING & DETECTIE

Het NCSC omschrijft²⁶ het belang van monitoring en detectie en geeft *best practices* omtrent de implementatie ervan. Primair dient het netwerkverkeer gelogd en gemonitord te worden en voorzien van detectiemiddelen gezien dit het hart vormt waarop de systemen samenkomen. Vervolgens dient zich dit verder uitgebreid te worden richting alle gekoppelde VGS om de loggegevens veilig te stellen, analyse uit te kunnen voeren en snel aanvallen, verstoringen en afwijkingen te kunnen detecteren. Tenslotte moet er expertise zijn om deze gegevens te interpreteren en eventuele acties daarop te coördineren.

7.1 Tijdsynchronisatie

O	E7.1-01 • Alle VGS (inclusief componenten, netwerkcomponenten) synchroniseren hun systeemtijd met een betrouwbare bron voor tijdsynchronisatie, zodat de loggegevens eenduidig vergelijkbaar zijn. Tijdsynchronisatie dient op een veilige, cybersecure manier verkregen en geconfigureerd te worden. - Er is een betrouwbare tijdsynchronisatie voorziening die redundant (2 servers, op gescheiden netwerksegmenten) is uitgevoerd en met tussenkomst van een firewall alle VGS kan voorzien van tijdsynchronisatie. - Tijdsynchronisatie is zodanig ingericht dat het op basis van veilige koppelvlakken meerdere fysiek gescheiden netwerken kan voorzien. - Daar waar technisch mogelijk is verkeer versleuteld op basis van <i>Network Time Security</i> (NTS). - Er is sprake van betrouwbare tijdsynchronisatie servers (bijv. Meinberg LANTIME M200/300, Microchip S600 of gelijkwaardig). - In air gapped situaties wordt dit vormgegeven met betrouwbare apparatuur op basis van satellieten en/of atoomklok. Er wordt <u>minimaal</u> gebruik gemaakt van 2 betrouwbare verschillende bronnen, bijvoorbeeld: 1. GNSS, bij voorkeur Galileo (EU) of GPS (VS). 2. DCF77 - In connected situaties kan bijvoorbeeld ook gebruik gemaakt worden van: ▪ Meinberg NTP Service (Duitsland) ▪ RIPE NCC (Europa) ▪ Centrale Rijksvoorziening (indien beschikbaar) Rechtstreekse synchronisatie met publieke internet-NTP-servers is niet toegestaan.
---	---

7.2 Logging & analyse

A	E7.2-01 • Opdrachtgever is gerechtigd hard- en/of softwarematige sensoren (<i>agents, probes</i>) te (laten) plaatsen/installeren in de netwerken/systemen van de betrokken VGS.
---	---

²⁶ NCSC Detectie in cybersecurity: <https://www.ncsc.nl/detectie/detectie-cybersecurity>



O	E7.2-02	- Systeem- en gebruikersactiviteiten worden minimaal gelogd conform de richtlijnen van de <i>JSCU Logging-essentials</i>²⁷. Op basis van een Risicoanalyse is vastgesteld welke aanvullende Logging noodzakelijk is. - Alle VGS (inclusief componenten, netwerkcomponenten en het systeem voor logging zelf,) worden gelogd binnen hun eigen omgeving: Het volgende wordt gelogd - Relevant netwerkverkeer (bijv. syslog). - Relevante events van detectiemiddelen. - Relevante loggegevens van VGS. - Relevant zijn daarbij: - Alle gegevens die inzage geven in de prestaties, fouten, verstoringen, afwijkingen, logische toegang, potentiële dreigingen, etc. - Loggegevens die bij incidenten de oorzaak middels een <i>root-cause analyse</i> inzichtelijk kunnen maken. - Zie ook eisen §7.4 Health Monitoring.
O	E7.2-03	- Een logregel bevat minimaal: - Actie die heeft plaatsgevonden. - Object waarop de gebeurtenis of handeling effect had - Resultaat van de gebeurtenis of handeling. - Oorsprong: het apparaat of de netwerkllocatie van waaruit de gebeurtenis of handeling in gang is gezet. - Actor: entiteit/proces die/dat de gebeurtenis in gang heeft gezet. - Tijdstempel: datum en tijdstip van de handeling.
O	E7.2-04	Een logregel bevat nooit gegevens die tot het doorbreken van de beveiliging kunnen leiden.
O	E7.2-05	Er is een overzicht van logbestanden die worden gegenereerd.
O	E7.2-06	Logbestanden zijn zodanig beschermd dat deze niet aangepast of gemanipuleerd kunnen worden. Het (automatisch) overschrijven of verwijderen van logbestanden wordt gelogd in een nieuw aangelegde log.
O	E7.2-07	(Tijdelijke) toegang tot de loggegevens is gereserveerd voor auditors, en voor het onderzoeken van fouten en incidenten. Hier dient bij toekenning van rechten rekening mee te worden gehouden.
R	E7.2-08	Het is mogelijk loggegevens en/of data rechtstreeks door te sturen naar een door Opdrachtgever aangewezen <i>Security Information Event Management</i> (SIEM) applicatie en/of <i>Security Operations Center</i> (SOC).
B	E7.2-09	Oneigenlijk wijzigen, verwijderen of pogingen daartoe van loggegevens worden zo snel mogelijk gemeld als informatiebeveiligingsincident.
B	E7.2-10	Loggegevens kunnen geëxporteerd worden in gangbare formats voor analyse.

7.3 Security Monitoring

R	E7.3-01	In geval van nieuwbouw, renovaties en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...) wordt een SOC-dienstverlener voor oplevering in overleg met Opdrachtgever geselecteerd, aangesloten en wordt een
---	---------	---

²⁷ <https://github.com/JSCU-NL/logging-essentials>



	overeenkomst voor de garantie- en beheerperiode overeengekomen. De SOC-dienstverlener dient nauw samen te werken met de Managed Service Provider (MSP) – deze tevens te monitoren – en primaire onderhoudspartij van de locatie.
O E7.3-02	- In geval van renovaties, nieuwbouw en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...) wordt in samenspraak met een SOC: - Een logcollector wordt ingericht, dat aangesloten kan worden op een SOC, zodanig dat dit geen vendor lockin kan vormen inzake de SOC dienstverlener. - Dat de security logsdata (Syslog, events, applicatie logs, device logs, ...) wordt doorgestuurd naar de logcollector, inzake: - Alle netwerkcomponenten (switches, firewalls, NAC, VPN gateways, ...). - Alle servers, clients, virtualisatieplatforms. - Alle <i>identity & access management</i> toepassingen (als Active Directory, LDAPS, RADIUS, NAC, PKI, MFA, PAM). - Alle VGS-applicaties met gebruikersaccounts en VGS-applicaties die als hoog of kritiek zijn geclassificeerd. - Back-up voorziening (o.a. mislukte back-ups/restores, gewijzigde credentials, eventuele ransomware detectie). - Tijdsynchronisatie servers (o.a. tijdafwijkingen, synchronisatiefouten). - Logs inzake logische toegang van alle IP controllers (als bijvoorbeeld deurcontrollers, gateways, PLC's, PAC's, DDC's, BACnet routers, OPC UA servers) en IP end points die in het zicht hangen (als bijvoorbeeld camera's, intercoms, codepanelen, bedienpanelen, biometrie scanners) voor als <u>kritiek</u> geclassificeerde VGS. - Logs inzake logische toegang van alle IP controllers en alle IP end points <u>buiten en in publiek</u> gebied die in het zicht hangen (als camera's, intercoms, codepanelen, bedienpanelen, biometrie scanners) voor als <u>hoog</u> geclassificeerde VGS. - Security data uit alle aanwezige cybersecurity oplossingen wordt doorgestuurd, waaronder in ieder geval: <i>Endpoint Detection and Response</i> (EDR) oplossing. <i>Network Detection and Response</i> (NDR) en/of OT-Monitoringsoplossing. <i>Intrusion detection and Response</i> (IDPS) oplossing. - Kwetsbaarheidsscanner. <i>Proxy</i> <i>Secure DNS</i>
R E7.3-03	- De Opdrachtnemer stemt met het SOC een risicogebaseerde set detectie-use-cases af, gebaseerd op de aanwezige VGS-componenten, de beschikbaar gestelde logbronnen en het actuele dreigingsbeeld. Deze use-cases worden minimaal jaarlijks en na significante wijzigingen of nieuwe dreigingsinformatie geëvalueerd en waar nodig aangepast. Dit bevat use cases inzake: - Logische toegang - Verdacht gebruik van privileged accounts. - Ongebruikelijke loginlocatie/-tijd (bij externe toegang). - Meerdere mislukte authenticaties. - Nieuwe of gewijzigde accounts met verhoogde rechten. - Configuratiewijzigingen



		▪ Firewall-, switch- of NAC-configuraties. ▪ Servers, clients hardening. ▪ PLC-, DDC- of controllerconfiguraties. - Detectie van malware of ransomware. - Hackpoging en/of lateral movement. - Detectie oneigenlijke apparaten (<i>rogue devices</i>). - Uitgeschakelde cybersecurity oplossingen. - Verlies van logging (logbron valt weg) of logcollector. - Grote tijdafwijkingen of synchronisatiefouten. - Firmware- of software-updates ▪ Buiten onderhoudsvensters of ongepland. ▪ Downgrade. - Ongebruikelijke netwerkverbindingen tussen zones. - Mislukte back-ups of restores. - Kwetsbare systemen met actieve exploitpogingen. - Communicatie met bekende malafide IP-adressen of domeinen.
B	E7.3-04	• Alle VGS inclusief het systeem voor logging zelf, worden gemonitord.
B	E7.3-05	• Afwijkingen die de cybersecurity raken worden middels alarmen tijdig gesignaleerd. Bijvoorbeeld: ongeoorloofde (fysieke) toegang, ongeoorloofd gebruik, afwijkende activiteiten (bandbreedte, rekenkracht, opslag, geheugen) en verstoringen (schrijffouten harddisk, wegvallen verbinding).
B	E7.3-06	• Afwijkingen die de cybersecurity raken worden tijdig opgevolgd.

7.4 Health Monitoring

De MSP kan idealiter een centraal beeld vormen van de gezondheid van het VGS landschap, middels o.a.:

- [Inzicht in prestaties en gebruik](#)
- [Trends en verschillen analyse](#)
- [Alert rapportage](#)

R	E7.4-01	• Inzicht in prestaties en gebruik: Opdrachtnemer levert op aanvraag de volgende rapportage: - Gebruik van systemen/<i>devices</i>/applicaties (performance/benutting/capaciteitsbeheer) ▪ Rekenkracht/Processor belasting (% CPU/GPU) ▪ Memory gebruik (% RAM) ▪ Opslag gebruik (% harddisks, SSD, NAS, SAN) ▪ Netwerkverkeer (% bandbreedte) ▪ Energieverbruik (kWh, relevant inzake <i>predictive maintenance</i>, duurzaamheid) - Gebruik van <i>devices</i> ▪ Gerealiseerde uptime (beschikbaarheid, betrouwbaarheid, binnen/buiten overeengekomen grenzen) ▪ Overzicht gebruiksduur, bijv. gebruiksduur/gebruiksuren (actief sinds, cumulatief) (technische levensduur, betrouwbaarheid)
---	---------	--



		▪ Overzicht intensiteit gebruik, bijv. #transacties, #meldingen, #(aan)sturingen (relevante informatie inzake <i>predictive maintenance</i>, storingen) - Overzicht licenties (geldigheidstermijnen, aantal in gebruik / aantal reserve) - Overzicht certificaten (uitgever / <i>certificate authority</i> (CA), geldigheidstermijnen, aantal in gebruik, aantal reserve (10%)) - Overzicht Accounts in gebruik (soorten en aantallen) - Overzicht Gebruik van <i>privileged accounts</i> (welke + tijden en duur)
R	E7.4-02	• Trend- en/of verschillenanalyse. Opdrachtnemer levert op aanvraag de volgende rapportage: - Fluctuaties en trends in de loop van de tijd (dag – week – maand – jaar)? Doel: capaciteitsbeheer (actie nodig?), inzicht in structurele problemen (storingen) - Wijzigingen inhoudelijk en met tijdstip gerapporteerd (Bijvoorbeeld hardware vervangen, updates doorgevoerd, instellingen gewijzigd, ...) - Wijzigingen t.a.v. belangrijke baselines (zie verderop), Doel: controleren of deze wijzigingen geautoriseerd zijn doorgevoerd (dan wel inherente risico's vormen).
R	E7.4-03	• Alerts. Opdrachtnemer levert op aanvraag de volgende rapportage: - Alarmen/cybersecurity incidenten (zie Cybersecurity triggers verderop), bijvoorbeeld: ▪ Ernstige risico's beschikbaarheid: stroomstoringen, failover server, uitval firewall, uitval <i>core-switch</i>, wegvallen kabel in backbone, ... ▪ Logs met hoge prioriteit, bijv. Syslog severity levels: 0 - Emergency, 1 - Alert, 2 – Critical, eventueel aangevuld met Syslog prioriteiten veld ▪ Ongeautoriseerde toegangen of pogingen daartoe, ingelogde Medewerker > 12 uur, accounts > 1 maand niet gebruikt - Fouten/storingen (schrijffouten, (ver)storingen, SMS-storingsmeldingen, Syslog <i>severity levels</i>: 3 - Error, 4 - Warning, eventueel aangevuld met Syslog-prioriteitenveld)? - Uitval <i>Devices/applicaties</i> (uitval, falen, crash, ...)? - Systemen die tegen maximale belasting aanlopen (capaciteit >80% alert, >90% kritisch) - Licenties waarvan het volume tegen de maximale capaciteit aanloopt. - Certificaten waarvan de geldigheid binnen 3 maanden verloopt.

7.5 Bewaking bewaartermijnen logging

Te handhaven bewaartijden van loggegevens zijn gedefinieerd in §2.5 Beschermen registraties en Bewaartermijnen.

R	E7.5-01	• Per type loggegevens is in de verschillende systemen de verplichte minimale en maximale standaard bewaartermijn ingesteld. Zie E2.5-03.
R	E7.5-02	• Gedeelten van logs kunnen separaat worden weggeschreven/gekopieerd en/of kunnen een langere bewaartermijn worden toegekend. Doel: bewijsvoering, <i>root cause analysis</i> Dit kan alleen met specifiek daartoe ingerichte en vrijgegeven <i>privileged accounts</i>.
B	E7.5-03	• Voor het handhaven van de overeengekomen bewaartermijnen zijn beheersmaatregelen opgesteld en geïmplementeerd.



7.6 Detectie & preventiemechanismen

Het doel van anti-malware, end point protection, indringingsdetectie- en Indringingspreventiesystemen (IDS/IPS) is het vroegtijdig signaleren en ingrijpen op digitale dreigingen.

O	E7.6-01	• <i>End point</i> detectie, waaronder Malware detectie, is geborgd binnen de netwerken en op de diverse <i>hosts</i> (servers/besturingssystemen) van de VGS.
O	E7.6-02	• <i>End point</i> detectie is zodanig zorgvuldig geconfigureerd dat goede bescherming wordt geboden en de operationele werking niet wordt verstoord (bijvoorbeeld door het uitsluiten van operationele bestanden waar veel bewerkingen op plaats vinden, het beperken tot <i>detect only</i> functionaliteit indien noodzakelijk en verdachte bestanden in quarantaine zetten zonder ze gelijk te verwijderen).
O	E7.6-03	• Er is een uitgewerkte en door Opdrachtgever goedgekeurde methode om detectie oplossingen te voorzien van de laatste handtekeningbestanden (<i>signatures</i>), met de volgende uitgangspunten: - Hard- & software inzake externe connectiviteit (firewalls, routers, gateways, ...) en DMZ zone worden real time actueel gehouden, VGS daarachter minimaal dagelijks. - VGS dat volledig air gapped is: minimaal maandelijks.
B	E7.6-04	• Periodiek (minimaal 4x per jaar) worden volledige systeemscans uitgevoerd o.b.v. bijgewerkte <i>anti-malware</i>. Systeemscans worden gepland op voor de operatie rustige momenten, waarbij de systemen qua performance gemonitord worden.
B	E7.6-05	• Bij detectie van malware of inbraak dient dit als een security incident gemeld en opgevolgd te worden.
O	E7.6-06	• Indringingsdetectie en -preventie (IDS/IPS) is volledige toegepast: - In geval van externe verbindingen. - In het geval van koppelvlakken met niet-vertrouwde zones.
O	E7.6-07	• Binnen de DMZ, op de <i>core firewall</i> en daarachter zijn deze detectiemechanismen professioneel ingericht, en goedgekeurd door Opdrachtgever.
O	E7.6-08	• Verderop in het netwerk en bij VGS is IDS/IPS weloverwogen toegepast, zonder dat operationele processen verstoord worden. - Gericht en voorzichtig binnen VGS-netwerken. - Gericht en voorzichtig als host IDS/IPS op servers en clients



8 STAATSGEHEIM

Als er sprake is van (raakvlakken met) staatsgeheime informatie zijn de eisen van toepassing zoals gesteld in de VIR-BI 2025²⁸ voor de Rijksoverheid en het Defensie Beveiligingsbeleid voor Defensie. Dit kan betrekking hebben op rubriceringen:

- Staatsgeheim CONFIDENTIEEL (Stg.C)
- Staatsgeheim – GEHEIM (Stg.G)
- Staatsgeheim – ZEER GEHEIM (Stg.ZG)

Deze rubricering heeft betrekking op de informatie (staatsgeheimen) en komen in hoofdlijnen overeen met de Te Beschermen Belangen (TBB's) in de ABRO die betrekking hebben op het beveiligingsregime van omgevingen in het kader van een opdracht: TBB3 (Stg.C), TBB2 (Stg.G) en TBB1 (Stg.ZG).

We onderscheiden de volgende situaties:

- Een Vastgoed Gebonden Systeem dat zich in een **ruimte** bevindt die als staatsgeheim is gerubriceerd.
- Een Vastgoed Gebonden Systeem dat zich in een **gebouw** bevindt dat als staatsgeheim is gerubriceerd.
- Een Vastgoed Gebonden Systeem dat als **systeem** als staatsgeheim is gerubriceerd.

8.1 VGS in staatsgeheime ruimte

Als een Vastgoed Gebonden Systeem zich in een staatsgeheime ruimte bevindt zijn de eisen van toepassing zoals gesteld in de VIR-BI 2025 voor de Rijksoverheid en het Defensie Beveiligingsbeleid voor Defensie (DBB). Specifieke aandacht dient hier uit te gaan naar

- Risicomanagement
- Fysieke beveiliging
- Tempestmaatregelen
- Afluisteren
- Systeem-inrichting en Cybersecurity

R	E8.1-01	• Het risicomanagement voor Vastgoed Gebonden Systemen in een staatsgeheime ruimte wordt gedurende het project en de beheerfase geborgd op basis van een in samenspraak met de Opdrachtgever en Gebruiker uitgevoerde risicoanalyse.
R	E8.1-02	• Fysieke beveiliging van VGS in een staatsgeheime ruimte is onderbouwd in een beveiligingsplan. Specifiek dient geborgd te worden dat deze systemen fysiek voldoende zijn beveiligd: - Apparatuur is geplaatst in beveiligde ruimtes (toegang, detectie, cameratoezicht). - Toegang tot racks of technische ruimtes wordt alleen verleend voor het specifieke (type) systeem waarvoor iemand verantwoordelijkheid draagt. Toegang is steeds onder begeleiding/toezicht.
O	E8.1-03	• Voor VGS in een staatsgeheime ruimte zijn de Tempest-maatregelen integraal goedgekeurd en afgestemd met adviseurs op het gebied van Tempest, Elektra, ICT en Cybersecurity conform de normering en beleidsadviezen van het VIR-BI, het Defensie Beveiligingsbeleid en relevante internationale standaarden.
O	E8.1-04	• Voor VGS in een staatsgeheime ruimte zijn maatregelen inzake afluisteren getroffen. Het kan hier gaan om afluisteren (geluid door wanden), afluisteren door aanstralen (trilling en ramen, frequenties in LED-lampen), reflectie van informatie (via beeldschermen, spiegelende oppervlakten). De maatregelen inzake afluisteren uitgewerkt in een plan dat

²⁸ VIR-BI 2025: <https://zoek.officielebekendmakingen.nl/stcrt-2025-30222.html>



	is afgestemd met adviseurs Bouwfysica, Beveiliging en Cybersecurity en integraal goedgekeurd.
O E8.1-05	- Voor VGS in een staatsgeheime ruimte zijn aanvullende beheersmaatregelen inrichting en cybersecurity genomen inzake de borging van (niet limitatief: - Informatiebeveiligingsbeleid en procedures (opzet, bestaan en werking) - Monitoring van VGS en Netwerken t.a.v. (digitale) dreigingen en (logische) toegang - Aparte/verdergaande fysieke en/of logische segmentatie, netwerksecurity en <i>hardening</i>. - De aanvullende maatregelen inrichting en cybersecurity zijn uitgewerkt in een plan dat is afgestemd met adviseur Cybersecurity en integraal goedgekeurd.

Specifieke aandachtspunten Vastgoed Gebonden Systeem in een staatsgeheime ruimte:

O E8.1-06	Afdoende afstand conform <i>Tempest</i> eisen omtrent bekabeling, leidingen, zendapparatuur (o.a. bedienpanelen in ruimten) is geborgd.
O E8.1-07	Data- en elektranetwerken zwart versus rood zijn fysiek gescheiden. Waar nodig zijn filters (elektra) en/of firewalls (cybersecurity) geplaatst.
O E8.1-08	- Zoveel mogelijk voorkomen door kans op elektromagnetische straling en/of af luisterrisico, door bijvoorbeeld: - Toepassing van glasvezel bekabeling i.p.v. koper. - Toepassing van flexibele rubber leidingen i.p.v. metalen. - Geluidsdemping in luchtkanalen.
O E8.1-09	- Het risico op af luisteren van microfoons is geborgd door afstand en/of organisatorische maatregelen) en is technisch voorkomen. Denk hierbij specifiek aan: - Intercomposten (spreek en luisterverbinding) - Omroepinstallatie ontruiming (gesproken woord), muziekinstallaties - Camera's (camerabeelden en mogelijkheid tot spreek en luisterverbinding) ...
O E8.1-10	- Er wordt géén gebruik gemaakt van draadloze communicatie voor bijvoorbeeld: - Bedienpanelen gebouwenbeheer (bijv. WiFi, Bluetooth) - Camera's (bijv. 4G, WiFi) 4G/5G modems ... - Apparatuur of modules of voor draadloze communicatie zijn <u>fysiek niet aanwezig</u>.
O E8.1-11	- In staatsgeheime ruimtes zijn mobiele <i>devices</i> onderhevig aan tempest en af luistervereisten. Hierbij is het uitgangspunt <i>Commercial Off-The-Shelf</i> (COTS) apparatuur toegepast wordt echter dat draadloze functies (als WiFi, Bluetooth, GPS, NFC), optische functies (infrarood), visuele en akoestische functies (als camera, microfoon, speakers), optische functies (status-leds) en sensoren (als locatiebepaling) zijn uitgeschakeld: - Waarvoor in het inkoopproces rekening mee wordt gehouden (achterwege laten functionaliteit, modulair). - Waar mogelijk dit hardware matig verwijderd wordt. - Overige zaken via hardening softwarematige uitgeschakeld worden, primair via de BIOS/EUFI. - Security monitoring oplossing dient dit te bewaken.



R	E8.1-12	• Gebruiker is gerechtigd om security scans uit te voeren van de toegepaste VGS componenten, ruimte, kabel tracés, etc., waaraan Opdrachtnemer haar medewerking verleend. - Vereisten inspecteerbaarheid worden voor oplevering afgestemd. - Een voorstel voor reserveonderdelen wordt uitgewerkt gezien in te brengen apparatuur eerst gescand moet worden en dit enkele weken doorlooptijd kan hebben.
B	E8.1-13	• VGS componenten die nieuw ingebracht moeten worden, vereisen een scan die enkele dagen tot weken aan doorlooptijd kan hebben. Opdrachtnemer voorziet in een voorraad van VGS componenten op locatie, zodanig dat uitval van een VGS component niet tot verstoring van de bedrijfsvoering kan leiden in geval van gemiddelde of hogere beschikbaarheid van de ruimte.

8.2 VGS in een staatsgeheim gebouw

Indien een Vastgoed Gebonden Systeem zich in een Staatsgeheim **gebouw** bevindt zijn de eisen van toepassing zoals gesteld in de VIR-BI 2025 voor de Rijksoverheid en het Defensie Beveiligingsbeleid voor Defensie. Hierbij gelden aanscherping van eisen t.a.v. de voorgaande paragraaf die in overleg met Opdrachtgever nadere invulling vereisen.

O	E8.2-01	• Voor VGS in een gebouw met rubricering Staatsgeheim geldt een verplichte toetsing aan de eisen gesteld onder §8.1 VGS in staatsgeheime ruimte op basis van de VIRBI 2025 in het geval van Rijksoverheid en het Defensie Beveiligingsbeleid in het geval van Defensie.
---	---------	---

Specifieke aandachtspunten Vastgoed Gebonden Systeem in een staatsgeheim gebouw:

O	E8.2-02	• VGS in een gebouw met rubricering Staatsgeheim communiceren niet met de buitenwereld en hebben geen externe verbindingen.
O	E8.2-03	• Een eenzijdig uitgaande verbinding voor monitoringdoeleinden (bijvoorbeeld alarmen, storingen, digitale dreigingen) naar een Rijksoverheid/Defensie dienst (of gelijkwaardig) kan worden toegestaan met expliciete toestemming en goedkeuring van Opdrachtgever.

8.3 VGS met rubricering STAATSGEHEIM

Het Rijksvastgoedbedrijf is ingericht op het werken tot maximaal Departementaal Vertrouwelijk en beschikt niet over de voorzieningen om VGS die als Staatgeheim worden gerubriceerd te ontwerpen, realiseren en/of beheren.

Advies: Rubriceer VGS tot maximaal Departementaal Vertrouwelijk. Stel vast waar zich eventueel vertrouwelijke of persoonsgegevens zich bevinden waarvoor een hogere rubricering overwogen wordt. Bekijk in hoeverre deze gegevens zijn te compartimenteren, te anonimiseren, etc ... teneinde voor het Vastgoed Gebonden Systeem de rubricering tot Departementaal Vertrouwelijk te kunnen beperken.

Voor VGS die als Staatsgeheim zijn gerubriceerd is het volgende van toepassing:

- De eindverantwoordelijkheid voor het systeem ligt bij de Gebruiker.
- De verantwoordelijkheid van het Rijksvastgoedbedrijf is beperkt tot een adviserende en/of coördinerende rol.
- De Gebruiker dient te voorzien in een passende werkomgeving.



Specifieke aandachtspunten voor als Staatsgeheim gerubriceerde VGS:

O	E8.3-01	Een Staatsgeheim gerubriceerd Vastgoed Gebonden Systeem heeft geen enkele externe verbinding (geen connectiviteit met buitenwereld).
O	E8.3-02	Aansluiting van andere locaties/objecten is de verantwoordelijkheid van de Gemandateerd Opdrachtgever.
O	E8.3-03	- Updates voor een Staatsgeheim gerubriceerde Vastgoed Gebonden Systeem kunnen conform §0 - Inrichting Update proces via externe connectiviteit worden verkregen. Scenario Air Gapped is hierbij van toepassing: Er mag geen directe koppeling bestaan tussen de bron van de updates en het domein van VGS.
R	E8.3-04	Staatsgeheim gerubriceerde VGS en alle daartoe behorende onderdelen zijn geregistreerd en hebben een duidelijke eigenaar.
T	E8.3-05	De maatregelen voor beveiliging van bijzondere informatie worden onder de verantwoordelijkheid van de BVA of de accreditatieautoriteit periodiek gecontroleerd.
T	E8.3-06	Gedurende de gehele levenscyclus van een Staatsgeheim gerubriceerd Vastgoed Gebonden Systeem worden periodieke audits, inspecties, reviews en tests uitgevoerd om te controleren of de beveiligingsmaatregelen effectief zijn. Deze controles worden uitgevoerd door deskundige specialisten die beschikken over de juiste onderzoeksmiddelen en beproefde onderzoeksmethoden.
B	E8.3-07	De verantwoordelijkheden en procedures voor het adequaat beheer en juist gebruik van de Vastgoed Gebonden-voorzieningen waarin bijzondere informatie wordt verwerkt, zijn vastgesteld.



9 CLOUDDIENSTEN

9.1 Cloud-architectuur

We zien dat steeds meer data in de cloud worden verrijkt, via dashboards en apps worden ontsloten en dat er vanuit de cloud ook commando's gegeven worden (tweewegverkeer). Dit vraagt zodoende aanvullende vereisten met betrekking tot een clouddienst alsmede extra aandacht voor uitgaande en inkomende verkeersstromen.

Dit hoofdstuk is vooralsnog indicatief en nog niet vastomlijnd gezien er nog geen vastgesteld 'VGS Cloudbeleid' is dat zich specifiek toespitst op VGS voor het Rijksvastgoedbedrijf en toepassing van cloud vergt afstemming van Opdrachtgever met haar gebruiker(s). Indien clouddiensten voor VGS worden overwogen moeten onderstaande eisen nader geconcretiseerd worden.

A	E9.1-01	- De clouddiensten dienen te voldoen aan de (nader te concretiseren) eisen gesteld in: - Cloudeisen vanuit de ABRO (ABRO H5) - Het Rijksbrede cloudbeleid (2026) - Het cloudbeleid van het Rijksvastgoedbedrijf
A	E9.1-02	Alle uitgangspunten in dit document – die dus voor Vastgoed Gebonden systemen op locatie (on-premise) vereist worden – zijn eveneens van toepassing op de clouddienst.
O	E9.1-03	De toepassingen van clouddiensten dienen expliciet kenbaar gemaakt te worden en vereisen schriftelijke goedkeuring van Opdrachtgever.
O	E9.1-04	Specifiek aandachtspunt is dat een aanvullende risicoanalyse wordt gemaakt met oog op de classificering van informatie en de afhankelijkheid van bepaalde functionaliteiten van de clouddienst en/of verbinding. Dit kan aanvullende beheersmaatregelen vereisen.
A	E9.1-05	Toepassing van clouddiensten in de private (rijks)cloud²⁹ hebben de voorkeur boven publieke cloud. Opdrachtgever behoudt het recht voor om hier gedurende de beheerfase naar over te stappen.
O	E9.1-06	Uitgangspunt bij een publieke cloud is dat de data bij voorkeur binnen Nederland blijft, maar te allen tijde de Europese Economische Ruimte (conform reikwijdte AVG) niet verlaat.
O	E9.1-07	De autonomie van de functionele werking van het VGS op locatie blijft te allen tijde geborgd, ook bij uitval verbinding of cloud, dan wel stopzetting van cloud dienstverlening.
O	E9.1-08	Clouddiensten zijn niet toegestaan voor een rubricering hoger dan Departementaal Vertrouwelijk.

Voordat een Cloudservice wordt afgenomen, moeten additioneel een aantal aspecten worden afgestemd. Ten aanzien van een SaaS-oplossing³⁰ zijn dit:

- De architectuur hoe de cloud omgeving is opgebouwd en welke andere clouddiensten eventueel verbonden zijn of diensten waarmee afhankelijkheden zijn.
- Welke wijze van data-ontsluiting zijn er en hoe zijn deze vormgegeven?
Bijv. dashboards, apps, API's, etc.

²⁹ Private cloud: clouddienst die uitsluitend gebruikt wordt door één organisatie (of Rijksoverheid) en/of die volledig geïsoleerd is van anderen, dit kan bijvoorbeeld in een overheidsdatacenter (ODC) of GovCloud omgeving.

³⁰ Gebaseerd op: 'Using Cloud Services Securely: Harnessing core controls', Information Security Forum, oktober 2019.



- Welke informatiebeveiligingscertificeringen zijn van toepassing op de cloud-omgeving en de onderliggende datacenters?

A	E9.1-09	• Het ecosysteem van eventuele andere verbonden clouddiensten en leveranciers waarbinnen de clouddienst opereert inclusief de daarmee gepaard gaande afhankelijkheden is inzichtelijk voor Opdrachtgever.
O	E9.1-10	• Het meest recente High-Level Design van de Cloudomgeving is goedgekeurd door Opdrachtgever.
O	E9.1-11	• Er zijn afspraken over de gevraagde informatiebeveiligingscertificeringen en assuranceverklaringen met betrekking tot de cloud-omgeving en de onderliggende datacenters.

9.2 Dataontsluiting

O	E9.2-01	• De geboden mogelijkheden van data-ontsluiting en de vormgeving daarvan zijn afgestemd met Opdrachtgever (dashboards, apps, API's, etc.).
R	E9.2-02	• Leverancier biedt inzicht in de roadmap en organiseert minimaal jaarlijks een Opdrachtgevers-overleg waarin klantwensen en nieuw te ontwikkelen functionaliteiten worden besproken.

9.3 Netwerkbeveiliging

O	E9.3-01	• TLS versleutelde verbindingen, of specifieke VPN of VPN site-to-site verbindingen, of wide area network (WAN) oplossing.
O	E9.3-02	• Beveiliging / Versleuteling conform NCSC-beveiligingsrichtlijnen³¹.
O	E9.3-03	• SSL report³² beschikbaar.
O	E9.3-04	• Data van Gebruiker wordt geïsoleerd en beschermd tegen andere omgevingen/Gebruikers/dreigingen middels netwerksegmentatie.
R	E9.3-05	• De Firewallconfiguratie van cloud service provider wordt actief toegepast en beheerd.

9.4 Logische toegang

O	E9.4-01	• Er zijn afspraken over de inregeling van Identiteit en toegangsbeheer met betrekking tot de toepassing van: - Aparte <i>credentials</i> per individuele gebruiker . - <i>On-premise</i> IAM-oplossingen. - IDentity as a service (IDaaS). - Eventuele andere dan wel of hybride oplossingen.
O	E9.4-02	• Cloudtoegang voor individuele gebruikers is ingericht op basis van <i>single sign-on</i> (SSO) en multi-factor authenticatie (MFA).
O	E9.4-03	• Rechten en rollen van beheerders zijn vastgesteld op basis van <i>least privilege</i> en vastgelegd in een Rechten- en rollenmatrix.
	E9.4-04	• Beheerders hebben standaard geen toegang tot gebruiksgegevens.

³¹ NCSC-beveiligingsrichtlijnen: <https://www.ncsc.nl/transport-layer-security-tls/ict-beveiligingsrichtlijnen-voor-transport-layer-security>

³² Een SSL labs test rapport zoals bijvoorbeeld [Qualys SSL Labs](https://www.ssllabs.com/index.html) : <https://www.ssllabs.com/index.html>



O		
R	E9.4-05	De hoeveelheid beheerders van Opdrachtnemer / Leverancier is beperkt tot een vastgesteld maximum.

9.5 Bescherming van data

A	E9.5-01	De dataopslag voldoet aan de Nederlandse en Europese wetgeving.
A	E9.5-02	Het HLD beschrijft duidelijk hoe de volgende zaken in lijn met de classificatie van de data zijn geborgd: - Beschikbaarheid, integriteit en vertrouwelijkheid van gebruiksgegevens. - Back-up proces. - Ontsluiting van data voor Opdrachtgever en/of de geautoriseerde individuele gebruikers.
O	E9.5-03	Verantwoorde versleuteling van data at rest.
O	E9.5-04	Voor gegevens met rubricering Departementaal Vertrouwelijk ligt het sleutelbeheer bij Opdrachtgever.
O	E9.5-05	Het HLD beschrijven duidelijk de genomen maatregelen om te detecteren of, en te voorkomen dat data ongeoorloofd de cloud-omgeving kan verlaten.

9.6 Security monitoring

Security monitoring is bij cloudoplossingen net zo belangrijk als bij de *on-premise* systemen, echter vragen ze voor een cloud-omgeving aparte invulling. Onderwerpen die hier terugkomen zijn:

- Kwetsbaarheidsmanagement, penetratietesten en code reviews.
- Security information and event management (SIEM).
- Security incident management.

O	E9.6-01	Gebeurtenissen en incidenten worden gelogd en gemonitord.
B	E9.6-02	Kwetsbaarheden worden actief in beeld gebracht en gemonitord.

9.7 Security assurance

Security assurance is een vereiste, waarbij o.a. periodieke audits en/of PEN-test rapportages gedeeld en beoordeeld dienen te worden.

O	E9.7-01	- De volgende aspecten zijn inzichtelijk en geborgd: Beschikbaarheid: De minimaal noodzakelijke beschikbaarheid van de clouddienst/verbinding (als percentage uptime). Resiliency: De weerbaarheid en robuustheid: - Welke onderdelen mogen falen en hoe vaak? - Welke onderdelen moeten dubbel zijn uitgevoerd. Performance/capaciteit: De omvang en snelheid van gegevensverwerking. Onderhoud: Afspraken over het onderhoud van de VGS. Duidelijkheid over eventuele onderhoudstaken van Opdrachtgever. Reversibiliteit: De mogelijkheid om de clouddienst te deactiveren en alleen van lokale voorzieningen gebruik te maken. Uitgangspunt is dat het functioneren van
---	---------	--



	Vastgoed Gebonden systemen nooit afhankelijk mag zijn van de clouddienst/verbinding. - Portabiliteit: De mogelijkheid om de gegevens te exporteren en/of naar een andere (rijks)clouddienst over te zetten. - Interoperabiliteit: Samenwerkingsmogelijkheden van de clouddienst met meerdere/andere VGS, locaties, (rijks)clouddiensten, etc.
--	--



10 FYSIEKE BEVEILIGING

Fysieke beveiliging wordt binnen RVB ingevuld door Adviseurs Beveiliging en databekabeling door ICT of Elektra adviseur. In dit hoofdstuk wordt uitsluitend ingegaan op specifieke aandachtspunten.

10.1 Fysieke toegang & begeleiding

O	E10.1-01	Fysieke toegang tot (ICT/technische) ruimte voor VGS is uitsluitend toegestaan voor daartoe geautoriseerde medewerkers.
---	----------	---

10.2 Ruimtes

Eisen voor de fysieke afscherming en conditionering van de ruimten waarin apparatuur is geplaatst:

O	E10.2-01	Alle componenten (behoudens <i>endpoints</i>) van VGS en Netwerken dienen in daarvoor geschikte ICT/technische ruimtes geplaatst te zijn, voorzien van beveiligingsmaatregelen in lijn met de te beschermen belangen, zonering en rubricering.
O	E10.2-02	Apparatuur is geplaatst in afzonderlijk afgesloten kasten (racks) voorzien van inbraakdetectie en een eigen slot en/of paslezer op de deuren.

10.3 Systemen

Eisen voor de fysieke en elektromagnetische afscherming van de apparatuur.

O	E10.3-01	Systemen zijn fysiek afdoende beschermd tegen interceptie, verstoring en/of manipulatie van data.
---	----------	---

10.4 Bekabeling

Eisen voor de fysieke en elektromagnetische afscherming van de bekabeling:

O	E10.4-01	Bekabeling is afdoende beschermd tegen interceptie, verstoring en/of manipulatie van data. Uitgangspunt is glasvezel of Cat 6A S/FTP.
---	----------	---



11 SECURITY CONFIGURATIE & PROCESSEN

11.1 Lifecycle management

Speerpunt in *Lifecycle*-management is de borging van het niveau van beveiliging gedurende de gehele levenscyclus van de software en hardware van de gebruikte apparaten.

O	E11.1-01	Alle door Opdrachtnemer geleverde hard- en softwarecomponenten worden minimaal 5 jaar ondersteund (<i>end-of-support</i>) en kunnen worden vervangen gedurende minimaal de afgegeven technische levensduur (<i>end-of-life</i>) van het Vastgoed Gebonden Systeem waar deze deel van uitmaken.
R	E11.1-02	Opdrachtnemer zet geen producten in die <i>end-of-sale</i> zijn.

11.2 Asset- & configuratiemanagement

Een correcte en complete registratie van VGS in een Configuratie Management Database (CMDB) is van groot belang voor het kunnen bewaken van de cybersecurity van deze systemen. De in de CMDB vastgelegde gegevens zijn ook de basis voor Lifecycle management en input voor de meerjarenonderhoud- en investeringsplanning (MOIP).

V	E11.2-01	De Opdrachtnemer stelt bij de oplevering van projecten de asset- en configuratieregistratie van alle Vastgoed Gebonden Systemen digitaal beschikbaar aan de Opdrachtgever in de vorm van een Configuratie Management Database (CMDB) conform het referentiedocument (0 Bijlage G : CMDB) of door Opdrachtgever aangeleverde geactualiseerde specificatie.
R	E11.2-02	De Opdrachtnemer verwerkt de asset- & configuratie gegevens in het document Cybersecurityplan(CSP) van de betreffende locatie(s) en registreert het in de door Opdrachtgever aangegeven applicatie.
B	E11.2-03	- De Opdrachtnemer actualiseert en controleert de asset- en configuratieregistratie door middel van (netwerk)scans op aanwezige hardware- en softwarecomponenten op de volgende momenten: - Direct na wijzigingen en updates - Jaarlijks - Voorafgaand aan de overdracht naar een andere beheerorganisatie.

Inventarisatie

Indien de asset- en configuratieregistratie niet volledig, juist en actueel is, dient dit alsnog inzichtelijk gemaakt te worden via een inventarisatie.

B	E11.2-04	Opdrachtnemer inventariseert, documenteert en registreert in de door Opdrachtgever aanwezen systemen, op verzoek van Opdrachtgever, de Vastgoed Gebonden Systemen en -netwerken, data(stromen) en koppelvlakken in detail. Zie Verwijzing 03: Instructie inventarisatie VGS en 0 Bijlage G : CMDB.
---	----------	---



11.3 Wijzigingsbeheer

B	E11.3-01	De Opdrachtnemer voert wijzigingen aan Vastgoed Gebonden Systemen en hun koppelvlakken uitsluitend uit op basis van een vooraf goedgekeurd wijzigingsplan dat minimaal een leveranciersverificatie, een testrapport conform de testvereisten, een rollback-plan, een back-upbevestiging en een afgestemde planning met de gebruikersorganisatie bevat.
B	E11.3-02	De opdrachtnemer verifieert na het doorvoeren van een wijziging dat deze succesvol is doorgevoerd.
B	E11.3-03	Indien een bepaalde update niet wordt doorgevoerd, legt Opdrachtnemer dit vast met onderbouwing en meldt dit bij Opdrachtgever.
B	E11.3-04	De opdrachtnemer actualiseert na een wijziging asset- en configuratiemanagement, relevante documentatie, risicodossier, CSP en eventuele verbeterplannen.
B	E11.3-05	De (ontwikkel), test, acceptatie (OTA) zijn gescheiden van de productieomgeving (P).
B	E11.3-06	In de productieomgeving wordt niet getest zonder expliciete, schriftelijke goedkeuring van de Opdrachtgever.

11.4 Kwetsbaarheden- en Patchmanagement

B	E11.4-01	Opdrachtnemer monitort externe bronnen inzake bekende kwetsbaarheden in de VGS in beheer en stuurt erop dat toeleveranciers ook proactief kwetsbaarheden kenbaar maken, zodat hier tijdig op geanticipeerd kan worden.
B	E11.4-02	Opdrachtnemer registreert kwetsbaarheden van de VGS en informeert Opdrachtgever conform overlegstructuur over deze kwetsbaarheden en de bijbehorende risico's.
B	E11.4-03	Opdrachtnemer verstrekt een Verbeterplan waarin wordt aangegeven hoe geconstateerde kwetsbaarheden kunnen worden opgelost.
R	E11.4-04	Het VGS-landschap is zodanig inricht dat voldaan kan worden aan de update- & patchmanagent eisen in deze paragraaf.
B	E11.4-05	Opdrachtnemer voert het updateproces uit (reguliere updates, upgrades en security patches van systemen, ...) conform §11.3 Wijzigingsbeheer.
B	E11.4-06	Updates worden altijd vanuit gecertificeerde, vertrouwde bronnen verkregen en na downloaden wordt de integriteit geverifieerd (bijvoorbeeld automatisch of d.m.v. controle op basis van <i>hashes</i>).
B	E11.4-07	Updatebestanden worden voorafgaand aan implementatie op malware gescand.
B	E11.4-08	- Patchmanagement is zorgvuldig vormgegeven in afstemming met Opdrachtgever. - Voor reguliere updates is een vast schema opgesteld. - Voor incidentele updates is de termijn waarbinnen de update moet worden uitgevoerd o.b.v. de urgentie van een update (risicoafweging) vastgesteld. - Voor updates die niet binnen de gestelde termijn kunnen worden doorgevoerd, worden binnen de gestelde termijn compenserende maatregelen genomen. - Voor kwetsbaarheden in de context van het VGS-landschap met: - CVSS > 9, dienen direct mitigerende maatregelen genomen te worden en security patches doorgevoerd te worden binnen 3 kalenderdagen na vrijgave. - CVSS > 7, dienen direct mitigerende maatregelen genomen te worden en security patches doorgevoerd te worden binnen 7 kalenderdagen na vrijgave.



B	E11.4-09	- De volgende uitgangspunten dienen minimaal geborgd te worden: - Virtualisatieplatformen en besturingssystemen van air gapped systemen worden minimaal 2x per jaar van security patches voorzien en overige VGS minimaal 2 maandelijks. - Virtualisatieplatformen en en besturingssystemen van air gapped systemen worden minimaal 1x per jaar van updates voorzien en overige VGS minimaal per kwartaal. - Voor security patches en updates van VGS applicaties, firmware, etc. wordt het advies van de fabrikant gevolgd, wat doorgevoerd wordt op de geplande onderhoudsmomenten.
---	----------	--

11.5 Logisch toegangsbeheer

Ongewenste toegang tot VGS kan worden beperkt door effectief logisch toegangsbeheer: Gedegen [identificatie, authenticatie en autorisatie](#) mechanismen. Ook een goede implementatie van het [wachtwoordbeleid](#) is van belang: afdwingen van gedegen wachtwoorden, het actief wijzigen van default wachtwoorden, gebruik van multi-factor authenticatie (MFA) waar nodig, gebruik van *single-sign-on* (SSO) waar mogelijk, aanvullende maatregelen voor *privileged* gebruikers en het gebruik van een wachtwoordkluis.

O	E11.5-01	Logische toegang wordt verleend op basis van identificatie, authenticatie, autorisatie en logging voldoet aan auditvereisten.
O	E11.5-02	De uitgangspunten voor autorisaties zijn gebaseerd op het <i>least privilege</i> principe en op basis van <i>need-to-know</i>.
O	E11.5-03	De Opdrachtnemer past voor alle systemen complexe wachtwoorden toe bestaande uit minimaal 15 karakters – jaarlijks te veranderen – bestaande uit een combinatie van hoofdletters, kleine letters, cijfers en speciale tekens, waarbij technische afwijkingen vooraf schriftelijk door de Opdrachtgever moeten zijn goedgekeurd inclusief bijbehorende compenserende maatregelen.
O	E11.5-04	Het gebruik van toegangspas (Rijkspas) of andere chipcardtokens is toegestaan om in te loggen in plaat van een wachtwoord, mits gecombineerd met een minimaal 4-cijferige pincode en dat bij het verwijderen van de toegangspas/chipcardtoken de toegangsbeveiligingsvergrendeling automatisch wordt geactiveerd.
O	E11.5-05	De Opdrachtnemer past voor gebruikers accounts op individueel niveau toe en richt voor gebruikers met toegang tot meerdere systemen Single Sign-On (SSO) in dat herleidbaar is tot de individuele gebruiker, tenzij vooraf schriftelijk anders is overeengekomen met de Opdrachtgever.
O	E11.5-06	Wachtwoorden zijn versleuteld en <i>hashed</i> opgeslagen en indien technisch mogelijk worden voorafgaand aan <i>hashing</i> 'salting' (unieke toevoeging per wachtwoord opgeslagen in database) en 'peppering' (algemene toevoeging per wachtwoord elders opgeslagen) mechanismen toegepast.
R	E11.5-07	De Opdrachtnemer definieert en implementeert rollen en bijbehorende rechten in VGS en legt deze vast in een Rechten en Rollen matrix per Vastgoed Gebonden Systeem en legt dit ter goedkeuring voor aan Opdrachtgever.
B	E11.5-08	De Opdrachtnemer gebruikt uitsluitend generieke accounts of groepsaccounts na voorafgaande schriftelijke onderbouwing en expliciete toestemming van de Opdrachtgever.



B	E11.5-09	Alle wachtwoorden worden uitsluitend opgeslagen in een beveiligde en geautoriseerde digitale wachtwoordkluis, behoudens de noodprocedure die in een fysieke kluis wordt bewaard.
B	E11.5-10	De Opdrachtnemer voorziet individuele gebruikers en beheerders van de VGS van duidelijke instructies (hetgeen ook meegenomen dient te worden bij bewustwording/training) omtrent de werkwijze en de gewenste toepassing van logisch toegangsbeheer.

Wachtwoorden van devices

R	E11.5-11	- Default (leveranciers)accounts bij apparatuur (<i>devices</i>) worden verwijderd bij oplevering. Elk device wordt voorzien van een certificaat of een uniek, random, complex wachtwoord, met de volgende eigenschappen: ≥ 12 karakters: jaarlijks te veranderen, of ≥ 15 karakters: eens in de 3 jaar te veranderen, of ≥ 20 karakters: eens in de 5 jaar te veranderen Genoemde aantallen kunnen in de loop der tijd worden herzien.
B	E11.5-12	De Opdrachtnemer beheert en verstrekt de wachtwoorden van devices aan een door de Opdrachtgever vooraf geautoriseerde selectie van personen, waarbij de Opdrachtnemer deze wachtwoorden wijzigt bij functiemutaties of uitdiensttreding van de geautoriseerde personen.
B	E11.5-13	De Opdrachtnemer controleert bij firmware updates dat niet wordt teruggevallen naar een default account en/of wachtwoord.

Privileged Access Management (PAM)

*Privileged accounts hebben aanzienlijk meer rechten (bijvoorbeeld **administrators** en **super users**) of gebruiker met specifieke rechten (bijvoorbeeld **auditors**, gebruikers die camerabeelden mogen exporten, gebruikers rechten mogen geven). Daarom gelden hiervoor strengere eisen.*

O	E11.5-14	Beheertaken (administrator accounts) zijn verdeeld over meerdere accounts (ook als deze bij één persoon zijn belegd) om kritieke functies te kunnen scheiden.
O	E11.5-15	Muteren en/of verwijderen van logbestanden is alleen mogelijk met een separaat account waarin geen andere beheertaken mogelijk zijn.
O	E11.5-16	De Opdrachtnemer past voor privileged access accounts complexe wachtwoorden toe van minimaal 15 karakters in combinatie met tweefactorauthenticatie (2FA), of minimaal 20 karakters indien 2FA technisch niet mogelijk is.

Noodprocedures

R	E11.5-17	De Opdrachtnemer stelt in afstemming met de Opdrachtgever en/of de Gebruiker noodprocedures op. In ieder geval voor het herstellen van onverwacht geweigerde toegang tot kritische functies en voor het gecontroleerd toekennen van noodbevoegdheden voor kritieke handelingen in noodsituaties.
B	E11.5-18	De Opdrachtnemer vervangt de gebruikte inloggegevens uiterlijk de eerstvolgende werkdag na afronding van testactiviteiten of incidenteel gebruik.
B	E11.5-19	De Opdrachtnemer test de noodprocedures minimaal één keer per kalenderjaar.



11.6 Back-up en herstel

Voor een solide bedrijfscontinuïteit is het betrouwbaar inrichten van back-up en herstel (*recovery*) van belang. Er worden de volgende **typen data** onderscheiden met betrekking tot back-up:

- **Applicatie/toepassing:** alle data die direct aan de applicatie is gerelateerd (TCS, GBS, PZI, ...).
 - Applicatie data: alle data die in het systeem is opgeslagen (data van pashouders, camerabeelden, gebruikersdata, logische toegang, ...)
 - Applicatie log-data: alle gelogde data t.b.v. de applicatie (meldingen, alarmen, storingen, mutaties, pasgebruik, ...)
 - Applicatie en/of device configuratiedata: specifieke instellingen van de software van de applicatie (regels, alarmtriggers, sluisfuncties...) en in de firmware van devices (deurcontrollers, intercoms, camera's, etc.)
- **Systeem/netwerk:** dit zijn alle instellingen van de ICT-componenten, besturingssystemen, virtualisatie platforms, netwerken ... ten behoeve van applicaties, waaronder:
 - Software: alle software als besturingssystemen, virtualisatie platforms, ondersteunende applicaties, waarbij ook licenties en certificaten meegenomen moeten worden.
 - Systeem- & netwerkconfiguraties: configuratie van het besturingssysteem, netwerkcomponenten, virtualisatie platforms, ...
 - Systeem & netwerk log-data: alle relevante data relevant t.a.v. de performance en beveiliging van de systemen.

NB: De software en configuraties kunnen ook geborgd worden middels images, installatie scripts, snapshots, etc.

O	E11.6-01	• De volgende specifieke uitgangspunten zijn van toepassing: - <i>Recovery Point Objective</i> (RPO): dataverlies bedraagt maximaal 24 uur. - <i>Recovery Time Objective</i> (RTO): hersteltijd is maximaal 4 uur.
O	E11.6-02	• Server en clients worden volledig geback-up't (configuratie, data en log-data van virtualisatieplatforms, besturingssystemen, applicaties, etc.) volgens het GFS-rotatieschema (Grandfather, Father, Son): - Dagelijks (7 dagen per week) een volledige back-up. - Wekelijks een back-up te bewaren (4x). - Maandelijks een back-up van elke maand te bewaren (12x, tot 12 maanden terug).
R	E11.6-03	• De Opdrachtnemer stelt in afstemming met de Opdrachtgever en de Gebruiker per Vastgoed Gebonden Systeem een back-up- en herstelplan op waarin de herstelprocedures en de expliciete afbakening van uitgesloten onderdelen zijn vastgelegd.
R	E11.6-04	• Server en clients back-ups worden gepland en geautomatiseerd uitgevoerd op een 'verbonden' systeem met minimaal de volgende functionaliteit. - Automatisch verificatie en logging van back-ups, zodat automatisch controle plaatsvindt dat een back-up succesvol is. Foutmeldingen worden duidelijk en direct gerapporteerd. - Veiligstelling van systeemconfiguraties, functionele (applicatie) data en systeemdta (logbestanden). - Toepassing van door Opdrachtgever gestelde maximale bewaartermijnen. - Bescherming van Back-ups tegen verlies, beschadiging, wijziging en oneigenlijke toegang in fysieke, technisch/logische en organisatorische zin. Specifieke bescherming tegen cyberdreigingen als een <i>ransomware</i> aanval.



		- Back-up data <i>in transit</i> en <i>at rest</i> zijn versleuteld conform veilige en toereikende encryptie. - Herstel is zowel selectief (per bestand/component) als volledig mogelijk.
B	E11.6-05	• Alle configuraties van systemen, netwerken, applicaties en devices (die niet zonder configuratie werkend aangesloten worden) geldt dat zij: - Kunnen terugvallen op minimaal 3 oudere configuraties. - Kunnen minimaal 6 maanden terug in de tijd gaan voor alle configuraties in die periode (in geval van veel wijzigingen in een korte periode). Deze back-up's worden geplaatst op systemen die in het GFS-rotatieschema worden meegenomen.
B	E11.6-06	• De Opdrachtnemer bewaart back-ups minimaal één keer per twee maanden op een offline medium in een door de Opdrachtgever daartoe aangewezen brandwerende kluis op locatie, dan wel de back-up voorziening voorziet in <i>immutable</i> back-ups in een andere ICT- of technische ruimte.
B	E11.6-07	• Bij elke wijziging (geplande configuratie wijziging, update van software/firmware/applicaties, etc.) worden - <u>Voorafgaand</u> aan de werkzaamheden volledige back-ups gemaakt, separaat voor systemen/applicaties; configuratie en data. - <u>Achteraf</u> (na succesvolle wijziging) volledige back-ups gemaakt, separaat voor systemen/applicaties; configuratie en data. - De laatste volledige back-up wordt (tevens) op een offline medium bewaard in een daartoe aangewezen brandwerende kluis op locatie.
B	E11.6-08	• De Opdrachtnemer test de herstelprocedures bij oplevering en vervolgens minimaal één keer per kalenderjaar in afstemming met de Opdrachtgever en/of de Gebruiker, waarbij de testen via een vooraf goedgekeurd en risicogestuurd testplan zonder verstoring van de productieomgeving worden uitgevoerd.

11.7 Incident- & response management

B	E11.7-01	• Opdrachtnemer verleent haar medewerking aan het opstellen en implementeren van Cybersecurity incident- & response management in samenspraak met Opdrachtgever en Gebruiker.
B	E11.7-02	• In het geval er een Managed Service Provider (MSP) en een Security Operations Center (SOC) zijn aangesloten conform VGS CS Architectuur: - Is de MSP het eerste aanspreekpunt voor storingsanalyse en/of <i>root cause analyse</i>, alvorens onderliggende VGS-leveranciers worden ingeschakeld. - Ondersteund het SOC het incidentmanagement proces.
B	E11.7-03	• Opdrachtnemer doet binnen 24 uur melding bij Opdrachtgever van privacy-incidenten, securityincidenten en kwetsbaarheden die hebben geleid tot of zouden hebben kunnen leiden tot een vermoedelijke of opzettelijke inbreuk op de beschikbaarheid, vertrouwelijkheid of integriteit van informatieverwerkende systemen, waaronder de VGS in beheer.
		• Het is aan Opdrachtgever om te bepalen of daar (i.v.m. meldingsplicht binnen 24 en 72 uur) melding van gemaakt wordt bij de betreffende autoriteit of toezichthouder.
R	E11.7-04	• De Opdrachtnemer verleent volledige en tijdige medewerking aan de identificatie, analyse, beheersing, afhandeling en evaluatie van (mogelijke) securityincidenten. Dit omvat ten minste:



	- Het identificeren, registreren en duiden van (mogelijke) securityincidenten. - Het analyseren, categoriseren en prioriteren (triage) van securityincidenten, waaronder: ▪ Het bepalen van de ernst, impact en prioriteit. ▪ Het vaststellen of sprake is van een meldingsplichtig privacy-incident of datalek. ▪ Het vaststellen of sprake is van een meldingsplichtig securityincident. - Het tijdig escaleren van incidenten naar de daarvoor aangewezen functionarissen, beheerders, leveranciers en/of het crisisteam. - Het uitvoeren van incidentresponsmaatregelen, waaronder: ▪ Het indammen van het incident en het beperken van verdere schade. ▪ Het forensisch verantwoord veiligstellen en aanleveren van bewijsmateriaal. ▪ Het treffen van tijdelijke mitigerende maatregelen indien direct herstel niet mogelijk is. - Het herstellen van systemen, connectiviteit, functionaliteit en gegevens naar een aantoonbaar veilige en normale bedrijfsvoering. - Het uitvoeren van een root cause analysis, inclusief het beoordelen of dezelfde oorzaak, kwetsbaarheid of dreiging ook elders binnen de omgeving aanwezig is. - Het doorvoeren van corrigerende en preventieve maatregelen, waaronder securitypatches, configuratiewijzigingen en overige verbetermaatregelen om herhaling van het incident te voorkomen. - Het verifiëren dat: ▪ Het incident volledig is afgehandeld. ▪ De oorzaak is weggenomen of beheerst. ▪ De getroffen maatregelen effectief zijn. ▪ De dienstverlening veilig kan worden hervat. - Het documenteren en evalueren van de incidentafhandeling, inclusief de vastgestelde root cause, de genomen maatregelen en de geïdentificeerde verbeterpunten (lessons learned).
--	--

11.8 Bedrijfscontinuïteit en disaster recovery plannen

R	E11.8-01	• De Opdrachtnemer stelt het <i>Disaster Recovery Plan</i> op (in lijn met door Opdrachtgever aangedragen best practices) en implementeert de nodige maatregelen in samenspraak met Opdrachtgever en Gebruiker. Deze maatregelen betreffen: - Beheersmaatregelen voor informatiebeveiliging, ondersteunende systemen en hulpmiddelen binnen bedrijfscontinuïteits- en ICT-continuïteitsplannen. - Processen om bestaande beheersmaatregelen voor informatiebeveiliging tijdens een verstoring in stand te houden. - Compenserende maatregelen voor beheersmaatregelen informatiebeveiliging die tijdens een verstoring niet kunnen worden gehandhaafd.
B	E11.8-02	• De Opdrachtnemer verleent onverkort medewerking aan simulaties, testen en trainingen op aangeven van Opdrachtgever.



12 ORGANISATIE & GOVERNANCE

12.1 Overlegstructuur en Rapportage

B	E12.1-01	Cybersecurity is een vast agendapunt in de diverse overleggen tussen Opdrachtnemer, Opdrachtgever en Gebruiker (zoals operationeel overleg, contractoverleg en jaarlijkse overleg als vervolg op de jaarlijkse inspectie). Cybersecurity wordt als apart onderwerp opgenomen in de verslaglegging. In deze overleggen wordt Cybersecurity steeds besproken met een ter zake kundig persoon namens de Opdrachtgever.
B	E12.1-02	De Opdrachtnemer rapporteert periodiek omtrent beheer VGS aan de Opdrachtgever in het Contractoverleg en als onderdeel van de Jaarrapportage naar aanleiding van de jaarlijkse inspectie, waarin minimaal wordt ingegaan op de onderwerpen in 0 Bijlage E : Specificatie Rapportage VGS.

12.2 Proces- & documentmanagement

T	E12.2-01	De Opdrachtnemer legt alle gebruikersprocessen, gebruikersprocedures en noodprocedures ter afstemming en toetsing voor aan de Opdrachtgever en de Gebruiker.
B	E12.2-02	De Opdrachtnemer evalueert jaarlijks in samenspraak met Opdrachtgever en de Gebruiker alle documentatie, beheerprocessen en procedures – met inbegrip van rollen en verantwoordelijkheden – en borgt de actualiteit daarvan, waarbij door Opdrachtgever als <i>best practice</i> aangereikte sjablonen als uitgangspunt worden gebruikt.
B	E12.2-03	De Opdrachtnemer actualiseert jaarlijks de in E13.1-01 en andere relevant geachte documenten, overlegt deze en ligt de wijzigingen toe (vervallen versus nieuw).
B	E12.2-04	De Opdrachtnemer bewaakt de gestelde normen en best practices door middel van een <i>Plan-Do-Check-Act</i> (PDCA)-cyclus en houdt beheerprocessen, (beheer)procedures en documentatie actueel, waarbij de resultaten periodiek ter afstemming aan de Opdrachtgever worden voorgelegd.

12.3 Rollen en verantwoordelijkheden

O	E12.3-01	Opdrachtnemer implementeert door Opdrachtgever aangegeven beleid met betrekking tot scheiding van taken en bevoegdheden en treft passende maatregelen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
R	E12.3-02	De Opdrachtnemer legt de gedefinieerde rollen en verantwoordelijkheden voor VGS cybersecurity ter goedkeuring aan Opdrachtgever voor middels RASCI³³-overzichten en taakomschrijvingen.

³³ RASCI: Responsible (Verantwoordelijk), Accountable (Eindverantwoordelijk), Support (Ondersteunend), Consulted (Te raadplegen), Informed (Te informeren), Instructed (Te instrueren)



12.4 Personeelsmanagement

Screening en geheimhouding

Een aantal Gebruikers vraagt voor medewerkers die zich bezighouden met VGS om een geheimhoudingsverklaring en/of screening. Het beleid hieromtrent is vastgelegd in de VIRBI 2025 en in specifieke regelgeving van Gebruiker. De VIRBI 2025 kent de volgende screeningsniveaus:

- Verklaring Omtrent het Gedrag (VOG) t/m Departementaal Vertrouwelijk.
 - De categorieën zijn afhankelijk van de context en Gebruiker, dus per situatie af te stemmen.
 - Gebruikelijk voor het Rijksvastgoedbedrijf zijn categorieën VOG: 11, 12, 13, 41, 53, 71
- VGB³⁴-C (of vergelijkbaar) t/m Stg.C
- VGB-B (of vergelijkbaar) t/m Stg.G
- VGB-A (of vergelijkbaar) t/m Stg.ZG

A	E12.4-01	• Screening en geheimhouding van door Opdrachtnemer in te zetten personeel en/of derden zijn conform vigerend beleid van Rijksoverheid en Gebruiker, en sluiten aan op de te beschermen belangen (TBB).
---	----------	---

In en uit dienst

Bij in- en uitdienstprocedures geeft Opdrachtnemer specifiek aandacht aan informatiebeveiliging.

R	E12.4-02	• De Opdrachtnemer verleent tijdens het <i>onboarding</i> proces uitsluitend toegang tot systemen op basis van de vastgelegde rollen, verantwoordelijkheden en de principes van <i>least privilege</i> en <i>need-to-know</i>.
A	E12.4-03	• De Opdrachtnemer agendaert de geheimhoudingsplichten expliciet tijdens het exitgesprek met de medewerker die uit dienst treedt.
A	E12.4-04	• De Opdrachtnemer trekt alle verleende fysieke en logische toegangsrechten van een medewerker uiterlijk op de dag van uitdiensttreding volledig in.
B	E12.4-05	• De Opdrachtnemer voert bij de uitdiensttreding van een medewerker een risicoanalyse uit op de opgebouwde kennis van Vastgoed Gebonden Systemen en minimaliseert de geïdentificeerde risico's direct door passende maatregelen te nemen. Denk aan: bekendheid met wachtwoorden, IP-locaties, bepaalde procedures, etc.

12.5 Bewustwording en training

T	E12.5-01	• De Opdrachtnemer levert een gebruiksinstructie op en verzorgt een training over de systeemfunctionaliteiten en cybersecurity-aandachtspunten voor zowel de individuele gebruikers als de specifieke gebruikers/beheerders.
B	E12.5-02	• De Opdrachtnemer verzorgt voor alle medewerkers een cybersecurity-bewustwordings- en trainingsprogramma bij de aanvang van de opdracht, herhaalt dit minimaal één keer per kalenderjaar en stelt dit binnen dertig dagen na indiensttreding beschikbaar voor nieuwe medewerkers. Het bewustwordings- en trainingsprogramma behandelt ten minste: - Cybersecuritybeleid, rollen en verantwoordelijkheden. - Toegangsbeveiliging en veilig accountgebruik. - Herkenning van cyberdreigingen, waaronder phishing en social engineering.

³⁴ VBG: Verklaring van Geen Bezwaar



		- Veilig beheer en gebruik van VGS en bijbehorende beheeromgevingen. - Het herkennen en melden van beveiligingsincidenten en kwetsbaarheden. - Het veilig omgaan met vertrouwelijke informatie. - Gedragscode, acceptabel en verantwoord gebruik middelen en systemen.
B	E12.5-03	• De Opdrachtnemer voldoet aan de voorschriften voor acceptabel gebruik en de meldingsprocedure voor cybersecurity-incidenten zoals specifiek vastgelegd in 0 Bijlage F : Do's en don'ts acceptabel gebruik.

12.6 Transport van gegevens

B	E12.6-01	• Gegevens die de fysieke locatie verlaten (bedraad, draadloos of via media) zijn expliciet gedocumenteerd en hebben goedkeuring van Opdrachtgever. Gegevens mogen uitsluitend via de door Opdrachtgever goedgekeurde netwerkinfrastructuur of media de fysieke locatie verlaten.
B	E12.6-02	• Transport en/of communicatie van bijzondere informatie vindt plaats conform rubriceringsniveau volgens de vereisten zoals gesteld in VIRBI (art. 7, H6) en ABRO (3.5 t/m 3.8).

12.7 Vernietiging van gegevens

B	E12.7-01	• Vernietiging van gegevens/informatie vindt plaats conform de eisen behorend bij het classificatie-/rubriceringsniveau (zie VIRBI H6, ABRO bijlage 8). Gegevens worden vernietigd: - Op eerste verzoek van Opdrachtgever. - Bij het verstrijken van bewaartermijnen. - Na ontbinding van de overeenkomst (conform exit plan). - Conform overeengekomen contractuele bepalingen. - Bij afvoer van een systeem of componenten (bijv. bij uitfasering, vervanging, defect raken). - Opdrachtnemer verstrekt bewijs van vernietiging.
---	----------	--

12.8 Contract- & leveranciersmanagement

B	E12.8-01	• De Opdrachtnemer zet voor het onderhoud van de systemen uitsluitend medewerkers en ingeschakelde derden in van wie de bekwaamheid vooraf is aangetoond middels geldige, relevante certificaten of erkende opleidingsdiploma's.
---	----------	--



13 ASSURANCE, TOETSING & RAPPORTAGE

13.1 Certificeringen/audits organisatie, systemen & producten

Certificeringen en/of auditrapportages omtrent de betrokken organisaties en/of ingezette systemen/componenten dragen bij aan de cybersecurity assurance en zijn in het CSP vermeld en wordt naar de betreffende bijlagen verwezen. Het gaat hier om certificeringen/audits die op voorhand bekend zijn, waarbij een beeld gevormd kan worden van de *security posture* en die bijdraagt aan de aantoonbaarheid daarvan. In het project wordt voor de toegepaste VGS een pen-test afgeroepen en tijdens de instandhouding worden periodiek audits verlangd.

T	E13.1-01 • De Opdrachtnemer voegt, indien beschikbaar, de volgende certificeringen en audit rapportage toe als bijlage en licht deze toe: - Gebruik van een intern Cybersecurity-framework en/of ISO 27001 certificering met Verklaring van Toepasselijkheid (<i>Statement of Applicability</i>) - IEC 62443 certificering inzake processen, systemen en/of componenten met vermelding van de <i>security levels</i>. - Audit rapportages als ISO 27001 Surveillance Audit rapporten en/of ISAE 3402 SOC2 Type II. - Penetratietesten op de getroffen systemen of op specifieke onderdelen daarvan inclusief opvolging bevindingen. - <i>Roadmap</i> van voorgenomen certificeringen, verklaringen en/of audits.
---	--

13.2 Testmomenten

Uiteraard is het van belang om vooraf de scope van de testomgeving en de tests af te stemmen. Het doel is om een zo'n realistisch mogelijk testopstelling te hebben, zodat eventuele aandachtspunten in een zo'n vroeg mogelijk stadium geadresseerd kunnen worden.

Tijdens de verschillende projectfasen zijn verificatie en validatie momenten ingebouwd, waarin de overeengekomen cybersecurity beheersmaatregelen aangetoond moeten worden en/of in de praktijk getoetst. Toetsing van documenten als het Cybersecurityplan (CSP) en verwijzingen vanuit deze documenten.

- Controle van certificeringen, auditrapportages, etc. om een beeld te vormen van security posture van de betrokken partijen en in te zetten producten/diensten.
- Fysieke inspecties van bijvoorbeeld geleverde apparatuur, componenten en opstelling. Om te verifiëren dat deze conform plannen zijn en dat e.e.a. netjes en professioneel uitgevoerd wordt.
- Meenemen van cybersecurity aspecten bij testmomenten als:
 - Factory Acceptance Test (FAT): een kleine maar representatieve opstelling op locatie van fabrikant of system integrator, met beperkte koppelingen met andere systemen of simulatie daarvan.
 - Site Acceptance Test (SAT): representatieve inbedrijfsstellingstest op locatie met inbegrip van koppelingen met andere systemen.
 - User Acceptance Test (UAT): functionele test en acceptatie door (of namens) de gebruiker.
- Security assurance middels bijvoorbeeld een pen-test om een aantal specifieke maatregelen te verifiëren en aandachtspunten vanuit een aanvalsperspectief te inzichtelijk te maken. Doorgaans te plannen na een SAT en voor oplevering.



T	E13.2-01	De Opdrachtnemer legt voor elke test vooraf een testplan met de daarin vastgelegde scope en testprotocollen ter goedkeuring voor aan de Opdrachtgever.
T	E13.2-02	In de testprotocollen: - Zijn relevante scenario's stapsgewijs uitgewerkt. - Is het verwachte resultaat van tests in termen van consequenties (impact) en (alarm)meldingen duidelijk omschreven. - Wordt getoetst of signalering door apparatuur eenduidig/begrijpelijk is voor beheerders en/of individuele gebruikers van de apparatuur en leidt tot afdoende opvolging. - Is een selectief aantal functionele testen opgenomen om verwachte resultaten te verifiëren. - Wordt getoetst of bij de afhandeling van storingen: - Duidelijk is hoe moet worden gehandeld. - Duidelijk is wat nodig is voor herstel. - Hoe geverifieerd wordt dat het herstel succesvol is.
T	E13.2-03	Tests vinden plaats in een testopstelling die representatief is voor de scope van de opdracht.
T	E13.2-04	Tests en testresultaten worden geverifieerd en afgetekend door Opdrachtgever.
T	E13.2-05	Tests resulteren in een testrapport waarin bevindingen en vervolgacties zijn gedefinieerd.
T	E13.2-06	- Tijdens testmomenten van proef- en/of live opstellingen worden de cybersecurity beheersmaatregelen die daarin zichtbaar gemaakt kunnen worden, meegenomen. Dit zal onder andere (niet limitatief) in het testen van: - Failover in geval van redundante systemen en/of andere redundantie. - Redundante voedingen/netwerkaansluitingen. - De impact van uitval van de diverse soorten netwerkcomponenten (bijv. <i>core switches/firewalls, distributie switches, server switches, access switches, KVM-switches</i>) getest wordt. Specifiek ook met oog op: - Impact van netwerkonderbreking op applicaties onderling (afhankelijkheden) en verwachte resultaat (bijv. autonome werking) - Impact op componenten in netwerk (<i>client – server – device</i> afhankelijkheden) - ICT/Cybersecurity voorzieningen (als besturingssystemen, virtualisatie platforms, <i>domain controllers, radius servers, (netwerk)beheerservers, rapportage/SIEM</i> toepassingen, ...) - Controle van netwerkbeveiliging als <i>port security, network access control</i> met oog op ontkoppelen/opnieuw koppelen <i>devices</i> en aansluiten <i>rogue devices</i>. - Hardening/inrichting van werkplekvoorzieningen vanuit gebruikshandelingen (en ontbreken van administrator rechten), blokkade van USB-poorten, ... - Aanwezigheid van bepaalde software (bijv. anti-malware) en/of actuele versies van software. - Uitval van endpoint devices. - Controle koppelvlakken, afhankelijkheden en communicatie met andere systemen. - Noodprocedures en de juiste werking daarvan.



13.3 Security Assurance

Onder *Security Assurance* wordt verstaan: het geheel aan activiteiten waarmee representatief en aantoonbaar wordt vastgesteld dat cybersecuritymaatregelen zijn ontworpen, geïmplementeerd en effectief functioneren. *Security Assurance* kan bestaan uit één of een combinatie van onder meer: inspecties, steekproeven, documentreviews, (self-)assessments, configuratie checks, controle op compliance, kwetsbaarheids-scans, technische audits, penetratietesten, red teaming of vergelijkbare beveiligingstoetsen.

T	E13.3-01	- De Opdrachtnemer stelt jaarlijks, in afstemming met de Opdrachtgever, een VGS <i>Security Assurance</i> plan op, wat in gaat op: - De uit te voeren <i>Security Assurance</i> activiteiten. - De reikwijdte. - De frequentie. - De toegepaste toetsingsmethoden. - De selectie van te toetsen systemen. - De planning. - De rapportage en opvolging van bevindingen. Het <i>Security Assurance</i> plan resulteert in een representatieve beoordeling van de naleving en effectiviteit van de overeengekomen cybersecurityeisen.
T	E13.3-02	De Opdrachtnemer voert gedurende het jaar het <i>Security Assurance</i> plan uit en rapporteert de bevindingen. Geconstateerde afwijkingen en risico's worden geanalyseerd, met de Opdrachtgever afgestemd, geregistreerd in het risicodossier en voorzien van passende beheersmaatregelen en opvolging.
T	E13.3-03	De Opdrachtnemer verleent onverkort en volledig medewerking aan audits (zie E1.6-07) uitgevoerd door ofwel in opdracht van Opdrachtgever.

13.4 Penetratietesten (pen-testen)

In de regel worden PEN-testen uitgevraagd door Opdrachtgever. In voorkomende gevallen kan de verantwoordelijkheid voor een PEN-test bij Opdrachtnemer liggen.

T	E13.4-01	In geval van renovaties, nieuwbouw en/of grootschalige (>80%) vervanging van een type VGS (beveiliging, gebouwbeheer, elektra, veiligheid, ...) en voor kritieke VGS wordt een pen-test uitgevoerd voorafgaand aan oplevering.
T	E13.4-02	PEN-testen worden door een onafhankelijk partij uitgevoerd. Hierover is vooraf afstemming tussen Opdrachtnemer en Opdrachtgever.
T	E13.4-03	PEN-testen worden aangevraagd en uitgevoerd volgens Instructie Pentesten. Zie Verwijzing 05: Instructie PEN-testen).
T	E13.4-04	De leverancier die de pen-test uitvoert is in bezit van Keurmerk Pentesten volgens certificatieschema Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en heeft een aantoonbaar track record.
T	E13.4-05	- PEN-tester (medewerker) is gekwalificeerd en gecertificeerd conform, of gelijkwaardig met: - Offensive Security Certified Professional (OSCP) - Licensed Penetration Tester Master (LPT) - GIAC Penetration Tester (GPEN) - GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) - CompTIA PenTest+



T	E13.4-06	• Pentester heeft aantoonbare kennis van technologieën toegepast in VGS (OT, ICT, Cloud, IIoT...).
T	E13.4-07	• Opdrachtgever bepaald welke informatie door Opdrachtnemer aangeleverd moet worden, waarbij voor de hand ligt dat dit: - Bij oplevering het CSP inclusief een selectief aantal bijlagen betreft. - Tijdens beheer het CSP inclusief een selectief aantal bijlagen betreft, maar ook resultaten uit het <i>Security Assurance</i> plan en/of aandachtspunten vanuit het risicoregister,



14 OVERDRACHT NAAR BEHEER

14.1 Overdracht naar nieuwe beheerorganisatie

Bij voorkomende projecten en contractwisselingen dient informatieoverdracht van Opdrachtnemer naar de nieuwe beheerorganisatie inzake cybersecurity en privacy geborgd te worden. Ook in de Garantieperiode dient beheer en onderhoud te worden uitgevoerd.

Beheer tijdens Garantieperiode

R	E14.1-01	- De Opdrachtnemer stelt in samenspraak met Opdrachtgever en Gebruiker een Beheerplan op voor de garantieperiode en overdracht naar beheer met de volgende uitgangspunten: <u>Beveiligingsupdates</u> worden afhankelijk van het risico zo snel mogelijk doorgevoerd. Met name in relatie met externe verbindingen dient hier hoge prioriteit aan gegeven te worden. <u>Beveiligingssoftware</u> ten behoeve van <i>malware- of intrusion-</i> detectie, frequent gecheckt op beschikbare updates van de handtekeningbestanden, zodat detectie van malware of aanvallen actueel blijft. Bij extern ontsloten systemen minimaal 6x per jaar, Bij <i>air-gapped</i> systemen minimaal 2x per jaar. <u>Software en firmware</u> worden periodiek bijgewerkt volgens vaste planningen met oog op toekomstige ondersteuning en eventueel additionele functionaliteiten.
R	E14.1-02	- Werkzaamheden tijdens de garantieperiode worden uitgevoerd conform de Beheereisen, waarbij specifiek aandacht voor borging van: - Lifecycle management - Asset- & configuratiemanagement - Risicomanagement - Wijzigingsbeheer - Beheer van technische kwetsbaarheden - Update en patchmanagement - Logisch toegangsbeheer - Back-up & herstel

Algemene eisen bij overdracht van beheer

R	E14.1-03	De Opdrachtnemer documenteert de overdracht en beveiligt deze documentatie adequaat volgens daartoe vastgestelde normen.
R	E14.1-04	- De Opdrachtnemer stelt een Overdrachtsplan op voor overdracht aan de beheerorganisatie en stemt dit af met Opdrachtgever, Gebruiker en de nieuwe beheerorganisatie. Doel van dit Overdrachtsplan is om tijdens de garantieperiode een soepele overgang te borgen. Dit Overdrachtsplan bevat in elk geval: - Specifieke afspraken met Opdrachtgever en Gebruiker met betrekking tot inrichting en uitvoering van beheerprocessen, en procedures. - Identificatie van kritische elementen, risico's en/of succesfactoren met oog op een goed functioneren van de systemen. - De specifieke afspraken met Opdrachtgever en Gebruiker met betrekking tot risico-acceptatie en mitigerende maatregelen.



R	E14.1-05	De Opdrachtnemer draagt het CSP met alle systeem- en netwerkdocumentatie volledig, compleet en conform daadwerkelijke realisatie over aan de beheerorganisatie.
R	E14.1-06	De Opdrachtnemer maakt inzichtelijk wat er vanuit producent/system integrator geadviseerd wordt om het beheer, onderhoud en de MeerjarenOnderhoudsInvesteringsPlanning (MOIP) optimaal vorm te geven t.a.v. updates, controles, monitoring, onderhoudswerkzaamheden, etc. voor de garantieperiode en de daaropvolgende beheerperiode.
R	E14.1-07	De Opdrachtnemer retourneert alle eerder verstrekte fysieke en elektronische bedrijfsmiddelen die het eigendom zijn van of toevertrouwd zijn aan de organisatie. Bij gebruik van persoonlijke apparatuur wordt alle relevante informatie getraceerd, aan de organisatie overgedragen en van de apparatuur verwijderd.



Bijlage A : Afkortingen & Begrippen

Daar waar afkortingen of definities niet duidelijk mochten zijn, wordt verwezen naar het [Cyber Woordenboek](#)³⁵ dat gepubliceerd is door [Cyberveilignederland.nl](#). Afkortingen en begrippen die daarin niet zijn te vinden, zijn hieronder opgenomen voor zover niet in de tekst reeds toegelicht.

Begrip	Toelichting
Actieve componenten	Componenten van VGS die actief zijn, in de zin dat ze rekenkracht of geheugen hebben. Bijvoorbeeld servers, PC's, controllers, camera's, bedienpanelen, sensoren, etc.
AIRCO	Air conditioning
Barrier	Een gecontroleerde scheiding tussen 2 netwerken, bijvoorbeeld een firewall, datadiode, etc.
Beheerorganisatie	Organisatie die belast is met (de aansturing van) het operationeel beheer van het vastgoed en daarmee ook de Vastgoed Gebonden Systemen.
Best practice	Bewezen effectieve methode, proces of activiteit die in een bepaalde context betere resultaten oplevert dan alternatieven.
Bijzondere Informatie	Informatie waar kennisname door niet-geautoriseerden nadelige gevolgen kan hebben voor de (vitale) belangen van de Nederlandse staat, voor zijn bondgenoten of voor één of meer ministeries. Bron: VIRBI 2025. Informatie, systemen, data, locaties die gerubriceerd is als Departementaal Vertrouwelijk (Dep.V.), Staatsgeheim-Confidentieel (Stg.C), Staatsgeheim-Geheim (Stg.G), Staatsgeheim-Zeer Geheim (Stg.ZG).
BIO	Baseline Informatiebeveiliging Overheid, huidige versie BIO2, versie 1.3 definitief (9 januari 2026).
Black box	Een systeem of component waarvan de interne werking, codering of structuur onzichtbaar, ontoegankelijk of onbegrijpelijk voor Opdrachtgever, en waarbij men zich alleen richt op de input en de output.
Blacklist	Een lijst van vooraf afgekeurde entiteiten. Alles wat op de lijst voorkomt is niet toegestaan (bijv. applicaties, services, protocollen, poorten, ...). Het tegenovergestelde van een Whitelist.
BMC	Brandmeldcentrale
BMI	Brandmeldinstallatie
Breach	Inbreuk. Compromittering van een systeem waarbij mogelijk data oneigenlijk is onttrokken.
CDV	Concerndienstverlener, de partij die namens de Gebruiker de facilitaire dienstverlening verzorgt.
Commissioning	Inbedrijfsname-toets
Comply or explain	Zie 'Pas toe of leg uit'-principe
COS	CameraObservatieSysteem
Credentials	Informatie die wordt gebruikt om de identiteit van een entiteit te verifiëren. Inloggegevens (gebruikersnaam, wachtwoord, en evt. extra factoren)
CS	CyberSecurity
CSR	Cybersecurity Raamwerk, zijnde dit document
CSP	Cybersecurityplan, template is separaat bijgevoegd
Cybersecurity posture	De algehele beveiligingssterkte en gereedheid van een organisatie om cyberbedreigingen te voorspellen, detecteren, erop te reageren en ervan te herstellen, hetgeen de mate van robuustheid en weerbaarheid van Vastgoed Gebonden Systemen weerspiegelt.
DAS	Distributed Antenna System: actief of passief antenne systeem dat voorziet in de gewenste in pandige dekking voor mobiele telefonie en andere communicatiemiddelen.
DBB	Defensie BeveiligingsBeleid
Default allow	Standaard toestaan. Dat alle verbindingen, services of functies standaard zijn toegestaan, en alleen de expliciet benoemde of bekende uitzonderingen worden geblokkeerd of geweigerd. Bijvoorbeeld toepassing in firewall.
Default deny	Standaard weigeren. Een beveiligingsconcept waarbij alle toegang, verkeer of acties standaard worden geweigerd, tenzij deze expliciet worden toegestaan door een vooraf gedefinieerde regel of configuratie. Bijvoorbeeld toepassing in firewall.
Defense in depth	Gelaagde, samenhangende beveiliging, teneinde weerbare en robuuste Systemen te realiseren.

³⁵ <https://cyberveilignederland.nl/woordenboek>



Begrip	Toelichting
<i>Disaster recovery</i>	<i>Disaster recovery</i> (noodherstel) is de strategie van een organisatie om het voortzetten van normale (of meest noodzakelijke) bedrijfsactiviteiten te garanderen na een ingrijpend voorval, zoals een natuurramp, stroomuitval, cyberaanval of een technische storing. In dit kader ligt de focus op het vastgoed en VGS die de primaire processen ondersteunen.
<i>Disaster Recovery Plan</i>	Een <i>Disaster Recovery Plan</i> behandelt gewoonlijk de inzet van procedures en tools die tot doel hebben gegevensverlies en downtime tot een minimum te beperken en tegelijkertijd bedrijfscontinuïteit te garanderen.
DMZ	<i>Demilitarized Zone</i> . Een apart gebied in een computernetwerk dat het interne netwerk scheidt van het Internet. Alle onderdelen van het netwerk die contact hebben met externe netwerken, zitten bij elkaar in dit gebied.
DPIA	<i>Data Protection Impact Assessment</i> . Engelse benaming voor de gegevensbeschermingseffectbeoordeling. Een analyse van de impact van een (voorgenomen) verwerkingsactiviteit op de privacy en persoonlijke levenssfeer personen. Voor specifieke gevallen is deze verplicht.
EMS	Energiemonitoringssysteem
<i>Fail safe</i>	Is een ontwerpprincipe waarbij een systeem of apparaat zodanig is ontworpen dat het bij het falen van een onderdeel, automatisch naar een vooraf gedefinieerde, veilige toestand overgaat, zonder schade aan te richten aan mensen, levens of eigendommen (ook wel faalveilig).
<i>Fail secure</i>	Een systeem of apparaat dat, in geval van een storing (zoals een stroomuitval), vergrendeld blijft en niet kan worden geopend.
Functionaris Gegevensbescherming (FG)	Ook wel Data Protection Officer (DPO) genoemd, een deskundige binnen een organisatie die onafhankelijk toezicht houdt op de naleving van de privacywetgeving.
GBS	Gebouwbeheersysteem
Gebruiker(s)	De organisatie(s) die het vastgoed afneemt/afnemen van het RVB en het vastgoed gebruiken. De Gemandateerd Opdrachtgever kan verschillende Gebruikers vertegenwoordigen. Zie ook 'individuele gebruiker'.
Gemandateerd Opdrachtgever (G)	Dit is een functionaris binnen de Rijksoverheid die de rol van opdrachtgever vervult, maar dit doet krachtens een toegekend mandaat. Voor Rijkskantoren is de Directoraat-generaal Digitalisering en Overheidsorganisatie (DGDOO) de Gemandateerd Opdrachtgever, die tevens kaderstellend is voor (bijzondere) specialities. Voor (bijzondere) specialities zijn Single Points of Contacts (SPC) als GO vanuit de gebruiker aangewezen. De Dienst Vastgoedmanagement (DVM) van het Defensie Ondersteuningscommando (DOSCO) treedt op als GO namens het ministerie van Defensie.
Gerubriceerde informatie	Zie Bijzondere Informatie
<i>Governance</i>	<i>Governance</i> betekent letterlijk 'bestuur' of 'beheersing'. Het omvat alle regels, structuren, processen en gedragscodes waarmee een organisatie wordt aangestuurd en gecontroleerd. Het doel is het creëren van transparantie, verantwoording en integriteit om zo de belangen van alle betrokkenen (stakeholders) te waarborgen. Dit behelst onder andere de verdeling van taken en verantwoordelijkheden op alle niveaus, maar ook elementen van de interne beheersorganisatie zoals functiescheiding, procedures en maatregelen voor de beheersing van bedrijfsprocessen en risico's.
High-level design	High-Level Design (HLD), of hoogwaardig ontwerp, is een architecturaal plan dat de algemene structuur van een softwaresysteem of product beschrijft, inclusief de belangrijkste componenten, hun interacties en hoe ze samenwerken. Het is een macro-niveau blauwdruk die zich richt op het "wat" en "hoe" op een hoog niveau, zonder in te gaan op de specifieke implementatiedetails, en dient als een roadmap en communicatiemiddel voor het hele projectteam.
HVAC	Heating, Ventilation and Air Conditioning, oftewel warmte opwekking, koude opwekking, luchtbehandeling en airco's.
Hypervisor	Virtualisatie platform
ICS	Intercomsysteem (verkeersintercom, cel-intercom)
ICT	Informatie communicatie technologie
IDS	Inbraakdetectiesysteem



Begrip	Toelichting
IDV	ICT-Dienstverlener die namens de Gebruiker optreedt. Hierbij kan een nuance gemaakt worden naar: IDV-P: Pand, degene die zorgdraagt voor de netwerkinfrastructuur voor de kantoorautomatisering van een locatie. IDV-G: Gebruiker, degene die zorgdraagt voor de ICT-werkplekvoorzieningen van de individuele gebruiker (laptops, beeldschermen, etc.).
<i>In control</i>	Een organisatie is 'in control' als zij afdoende kennis heeft van haar processen en afhankelijkheden, en op basis van zorgvuldige risico-afweging maatregelen treft om deze afdoende te beschermen.
Individuele gebruiker	Persoon die een VGS bedient/gebruikt.
Informatiesysteem	Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie. Informatiesystemen bestaan uit Informatietechnologie (IT) en/of Operationele Technologie (OT). Bron: VIRBI. Een Vastgoed Gebonden Systeem is een Informatiesysteem.
Informatietechnologie (IT)	IT richt zich op software, netwerken en computersystemen die digitale informatie, waaronder gegevens, genereren en verwerken. - Typische IT-taken omvatten netwerkbeheer, systeembeheer, softwareontwikkeling, databasemanagement en IT-ondersteuning.
(I)IoT	(I)IoT ofwel (<i>Industrial</i>) <i>Internet of Things</i> is een netwerk van slimme, via internet verbonden (industriële) apparaten en sensoren. Het verzamelt en analyseert data om (productie)processen te optimaliseren, automatisering te verhogen en efficiëntie te verbeteren Dit leidt tot efficiënter en effectiever onderhoud en beheer en lagere kosten.
Kioskmodus	Een functie waarmee apparaten, zoals tablets of computers, vergrendeld worden tot één of een specifieke groep apps, websites of functies. Dit beperkt de toegang van individuele gebruikers tot andere applicaties, instellingen en bestanden, waardoor het apparaat exclusief voor het beoogde, taakspecifieke doel wordt gebruikt.
<i>Low-level design</i>	Low-level design (LLD), ook wel Detailed-level design (DLD) is een gedetailleerde ontwerpfase in softwareontwikkeling die de kloof overbruggt tussen een algemeen, architecturaal High-Level Design en de feitelijke codering. Het focust zich op de interne structuur en werking van individuele componenten, door klassen, methoden, datastructuren, interfaces en algoritmen te specificeren. LLD's dienen als een blauwdruk voor ontwikkelaars, die gedetailleerde instructies bieden voor de implementatie, om zo een modulair, efficiënt, schaalbaar en onderhoudbaar systeem te garanderen.
MAI	Mobiel alarmsysteem
Malware	Samentrekking van <i>malicious software</i> (kwaadaardige software). Malware is de term die als generieke aanduiding wordt gebruikt voor onder andere virus, worm, adware, spyware en trojans.
NAC	Network Access Control, 802.1x
Netwerk	Het geheel aan verbindingen ten behoeve van de communicatie tussen de componenten van VGS.
NSA	Noodstroomaggregaat
OAI	OntruimingsAlarmInstallatie
Opdrachtgever	Het Rijksvastgoedbedrijf, contractpartij die de opdracht verstrekt. Zie definitie in het contract dat van toepassing is.
Opdrachtnemer	Contractpartij die de opdracht aanneemt. Zie definitie in het contract dat van toepassing is.
Operationele Technologie (OT):	Operationele Technologie (OT): OT verwijst naar technologie die wordt gebruikt om fysieke processen en activa aan te sturen en te monitoren, door middel van (<i>embedded</i>) systemen, software, netwerken, controllers, sensoren en actuatoren. OT wordt vaak toegepast voor de geautomatiseerde aansturing in industrieën zoals productie, energie, transport en communicatie. Dat betreft bijvoorbeeld beveiligingssystemen, brandmeldinstallaties, gebouwbeheersystemen, aansturingssystemen van pompen en pijpleidingen, machine-besturingssystemen, etc.
PAM	Zie <i>Privileged Access Management</i>
Pas toe of leg uit'-principe'	Bestuursprincipe (Engels: <i>comply or explain</i>) waarbij een organisatie verplicht is bepaalde standaarden of regels te volgen, tenzij gemotiveerd kan worden uitgelegd waarom dit niet wordt gedaan. Zie ook §3.2
Passieve componenten	Componenten van VGS die passief zijn (bijv. bekabeling), niet zijnde Actieve componenten.
<i>Privacy officer</i>	Een specialist die organisaties helpt te voldoen aan de privacywetgeving.



Begrip	Toelichting
<i>Privacy-by-Default</i>	Principe dat de instellingen van een product, app of dienst automatisch zo privacyvriendelijk mogelijk zijn ingesteld. Gebruikers hoeven zelf niets aan te passen om hun persoonsgegevens te beschermen; de "veiligste" optie is de standaard. Dit is een kernvereiste van de AVG/GDPR. Zie ook §3.2
<i>Privacy-by-Design</i>	Principe dat de bescherming van persoonsgegevens vanaf het allereerste begin van het ontwerp van producten, diensten of systemen wordt meegenomen, in plaats van achteraf. Dit betekent proactief inbouwen van dataminimalisatie, beveiliging en transparantie om aan de AVG te voldoen. Zie ook §3.2
<i>Privileged Access Management</i>	<i>Privileged Access Management</i> (PAM) richt zich op de controle, monitoring en bescherming van accounts met bijzondere rechten binnen een organisatie.
<i>Privileged Account</i>	Een <i>privileged account</i> verleent een gebruikers uitgebreidere of bijzondere rechten zoals <i>administrator</i> , <i>super user of auditor</i> . Een <i>privileged account</i> is een aantrekkelijk doelwit voor aanvallers vanwege hun vaak uitgebreide toegang tot vitale systemen en gevoelige gegevens.
PZI	Personen Zoek Installatie
<i>Ransomware</i>	Kwaadaardige software waarbij een slachtoffer afgeperst wordt, nadat zijn digitale systeem of de bestanden erop door versleuteling met een code op slot zijn gezet. De aanvaller biedt de code tegen betaling aan, zodat hij er weer bij kan. Maar zelfs dat is niet zeker. Ransomware is een samenvoeging van de woorden ransom (losgeld) en software.
RASCII	<i>Responsible</i> (Verantwoordelijk), <i>Accountable</i> (Eindverantwoordelijk), <i>Support</i> (Ondersteunend), <i>Consulted</i> (Te raadplegen), <i>Informed</i> (Te informeren), <i>Instructed</i> (Te instrueren)
<i>Roadmap</i>	Een globale planning van gewenste veranderingen.
<i>Rogue devices</i>	Apparatuur die geen onderdeel is van de gedocumenteerde/toegestane systemen.
<i>Root-cause analyse</i>	Oorzaken-analyse. Grondige analyse naar oorzaak in geval van een incident. Wordt gebruikt om vast te stellen wat de te nemen (herstel)maatregelen zijn om de oorzaak een probleem weg te nemen en na te gaan of er bij een incident geen andere digitale dreigingen en/of achterdeurtjes zijn ontstaan.
Rubriceren	Bepalen van het rubriceringsniveau en -duur van de bijzondere informatie op basis van de te verwachten nadelige gevolgen voor de vitale belangen van Nederland en de Nederlandse staat, voor zijn bondgenoten of voor één of meer ministeries als (een deel van) deze informatie bekend wordt bij niet-geautoriseerden. Bron: VIRBI.
Rubriceringsambtenaar	Ambtenaar bevoegd tot het vaststellen van rubriceringen, hiertoe gemandateerd door de secretaris-generaal. Bron: VIRBI.
RVB	Rijksvastgoedbedrijf
<i>Safety-by-Default</i>	Principe dat een product, dienst, app of systeem zo is ontworpen dat de instellingen automatisch op de veiligste optie staan, zonder dat de gebruiker hiervoor actie hoeft te ondernemen. Zie ook §3.2
<i>Safety-by-Design</i>	Principe dat veiligheidsrisico's al in de ontwerpfase van een product, systeem, bouwwerk of proces worden aangepakt, in plaats van achteraf. Dit proactieve principe voorkomt onveilige situaties bij uitvoering of gebruik door veiligheid vanaf de start in het DNA van het ontwerp te integreren. Zie ook §3.2
<i>Security Assurance</i>	Het geheel aan activiteiten waarmee representatief en aantoonbaar wordt vastgesteld dat cybersecuritymaatregelen zijn ontworpen, geïmplementeerd en effectief functioneren.
<i>Security levels</i>	In de IEC 62443 worden een aantal niveaus van Cybersecurity onderscheiden waarop systemen en/of componenten gecertificeerd kunnen worden.
<i>Security-by-Default</i>	Principe dat een systeem, app of dienst standaard zo <i>cybersecure</i> mogelijk is ingesteld. Gebruikers hoeven zelf geen beveiligingsinstellingen aan te passen om een veilig basisniveau te hebben. Zie ook §3.2
<i>Security-by-Design</i>	Principe dat beveiliging integraal vanaf het allereerste begin van het ontwikkelproces in software, systemen of producten wordt ingebouwd, in plaats van achteraf als een pleister. Het is een proactieve aanpak waarbij kwetsbaarheden in de ontwerpfase worden voorkomen, wat leidt tot robuustere en betrouwbaardere technologie. Zie ook §3.2
SMS	Security management systeem



Begrip	Toelichting
<i>Specialty of Bijzondere Specialty</i>	Een rijksgebouw waarvan de hoofdfunctie geen kantoorfunctie is vanwege speciale eisen vanuit het primair proces, óf een kantoorgebouw dat door deze specifieke eisen geen gedeelde huisvesting kan bieden aan organisaties buiten dat proces. Dit is gebaseerd op 3 pijlers: • Primair proces is leidend. • Geen reguliere kantoorfunctie. • Geen medegebruik mogelijk. Specialty stelsel: dit zijn functionele, taakgerichte panden die specifiek voor één operationele rijksdienst zijn ingericht. Denk hierbij aan: • Justitiële inrichtingen en detentiecentra (Dienst Justitiële Inrichtingen) • Rechtbanken en paleizen van justitie • Laboratoria en testfaciliteiten (zoals bijv. RIVM, NVWA) • Grensbewakingslocaties en douanepots Bijzondere specialities: Dit zijn objecten waarin niet-Rijksdiensten zijn gehuisvest, met een uniek maatschappelijk, historisch of representatief karakter waarvoor afwijkende sturings- en financieringsregels gelden. Bijvoorbeeld: • Hoge Colleges van Staat • Paleizen: Koninklijke paleizen die door de Staat ter beschikking worden gesteld. • Gedenknaalden. • Museumstelsel: Rijksmusea (zoals het Rijksmuseum of Mauritshuis). • Monumenten: Unieke historische monumenten en rijksgebouwen met een zware erfgoedstatus. • Koninklijke Bibliotheek.
Statement of Applicability	Verklaring van Toepasselijkheid. In veel certificeringen is een Verklaring van toepasselijkheid opgenomen. Hierin is vastgelegd op welke zaken en voor welke beheersmaatregelen (<i>controls</i>) van het onderliggende normenkader (<i>framework</i>) de certificering van toepassing is.
Stepping stone	Ook bekend als <i>jump server</i> : een streng beveiligde tussenmachine die beheerders toegang biedt tot afgeschermd netwerkzones. De <i>stepping stone</i> fungeert als een beveiligde gateway, vaak via SSH of RDP, om veilig beheer te faciliteren en het aanvalsoppervlak op kritieke infrastructuur te minimaliseren.
TCS	Toegangscontrolesysteem
Type systeem	Een VGS van hetzelfde type, zie §1.3, bijvoorbeeld beveiliging, gebouwbeheer, (brand)veiligheid, elektra, transport, ...
UPS	Uninterruptable Power Supply, no-break installatie
Vertrouwelijk	Alles met een classificatie vanaf 'Intern Vertrouwelijk'. Zie 0 'Bijlage B : Rubriceringsmatrix'.
VGB	Verklaring van Geen Bezwaar
VGS	Vastgoed Gebonden Systemen: Alle systemen en/of installaties die invulling geven aan functionaliteiten van het gebouw of terrein. Zie §1.3 Scope - Vastgoed Gebonden Systemen voor nadere toelichting.
VIR	Besluit Voorschrift Informatiebeveiliging Rijksdienst 2007
VIRBI	Besluit Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2025
VOG	Verklaring Omtrent het Gedrag
Whitelist	Een lijst van vooraf goedgekeurde entiteiten, terwijl de rest wordt geblokkeerd. Het tegenovergestelde van een blacklist.
Whitelist	Een lijst van vooraf goedgekeurde entiteiten, Alles op de lijst is toegestaan (applicaties, services, protocollen, poorten, ...). Alles wat niet op de lijst staat, wordt geblokkeerd. Het tegenovergestelde van een blacklist.
Wijziging	Een wijziging volgens de overeenkomst



Bijlage B : Rubriceringsmatrix

Binnen het Rijksvastgoedbedrijf wordt de volgende matrix gehanteerd.

				Bijzondere informatie (VIR-BI)			
Rijksvastgoedbedrijf				Ministeries	Staat en Bondgenoten		
Classificering	Open- baar	Intern Algemeen	Intern Vertrouwelijk	Dep.V.	Stg.C	Stg.G	Stg.ZG
Impact	Geen	Verlegenheid bij het RVB, klant(en), Gebruiker(s), personen	Schade aan de belangen van het RVB of RVB belanghebbende	Schade aan de belangen van de ministerie(s)	Schade aan vitale belangen van de Staat of bondgenoten	Ernstige schade aan vitale belangen van de Staat of bondgenoten	Zeer ernstige schade aan vitale belangen van de Staat of bondgenoten
Schadevorm							
1 Politieke / bestuurlijke schade	Geen	n.v.t.	Bestuurlijke schade aan organisatie bestuurders	Politieke schade aan een bewindspersoon	Aftreden bewindspersoon	Aftreden kabinet	Parlementaire crisis
2 Vertrouwen	Geen	Verlegenheid bij organisaties en personen	Vertrouwensverlies binnen/tussen/in organisatie(s) en tussen/in personen	Verlies van publiek respect	Publieke verontwaardiging	Verlies aan publiek vertrouwen	Structureel verlies aan publiek vertrouwen
3 Diplomatieke schade	Geen	n.v.t.	n.v.t.	Te herstellen door ambtelijke opschaling	Te herstellen door politieke opschaling	Externe bemiddeling noodzakelijk	Lange termijn schade t.o.v. vrienden / oorlog
4 Financiële schade	Geen	> €0	> € 5.000	> € 50 miljoen	> € 500 miljoen	> € 5 miljard	> € 50 miljard
5 Schade aan kritische processen	Geen	Geen	Kortdurend uitval van een kritisch proces RVB of RVB belanghebbende	Kortdurend uitval van een kritisch ministerieel proces	Kortdurend uitval van een vitaal statelijk proces	Langdurig uitval van een vitaal statelijk proces	Blijvend uitval van een vitaal statelijk proces

Niet alle waarden hebben een formele status. Zie voor meer details en nuances:

<https://www.digitaleoverheid.nl/document/gereedschap-rubriceren/>



Bijlage C : VERWIJZINGEN

Er zijn diverse documenten met meer gedetailleerde informatie en/of handvatten waar in dit document naar verwezen wordt. Deze zijn separaat opvraagbaar.

Verwijzing 01: Sjabloon Cybersecurityplan (CSP)

Verwijzing 02: VGS Business Impact overzicht

Verwijzing 03: Instructie inventarisatie VGS

Zie

- [Cybersecurity - Inzichtelijk maken systemen SJABLOON - CSP](#)

Verwijzing 04: Instructie classificatie VGS

Zie

- [VGS CS classificatie.docx](#)
- [VGS-Classificatie.xlsx](#)

Verwijzing 05: Instructie PEN-testen

Zie

- [Cybersecurity - Pentest Instructie X.x.docx](#)
- [Cybersecurity - Pentest Aanvraag SJABLOON.dotx](#)

Verwijzing 06: VGS CS Architectuur documenten

[Opvraagbaar](#)



Bijlage D : Voorbeeld ontwerp toepassing scrubber

VOORBEELD mogelijk ontwerp

- Een **geïsoleerde omgeving** is verbonden met de **buitenwereld**, teneinde:
 - Updates vanuit gecertificeerde bronnen te betrekken
 - Bestanden/configuraties van vooraf geautoriseerde leveranciers te ontvangen
 - De scrubber van actuele anti-malware e.d. te voorzien
 - De firewall achter de externe verbinding dient eveneens real time geactualiseerd te worden t.a.v. detectie van digitale dreigingen.
 - De omgeving zelf dient gemonitord te worden en alle servers dienen zelf ook van detectiesoftware voorzien te zijn en goed gehardend te zijn.
- Qua **werkwijze** kan een keuze gemaakt tussen:
 - Uitsluitend online ophalen/ontvangen van data en langs scrubber halen.
 - Alleen toepassing van een scrubber (en dat leverancier zelf met data op datadragers aankomen)
 - Combinatie van beide opties.

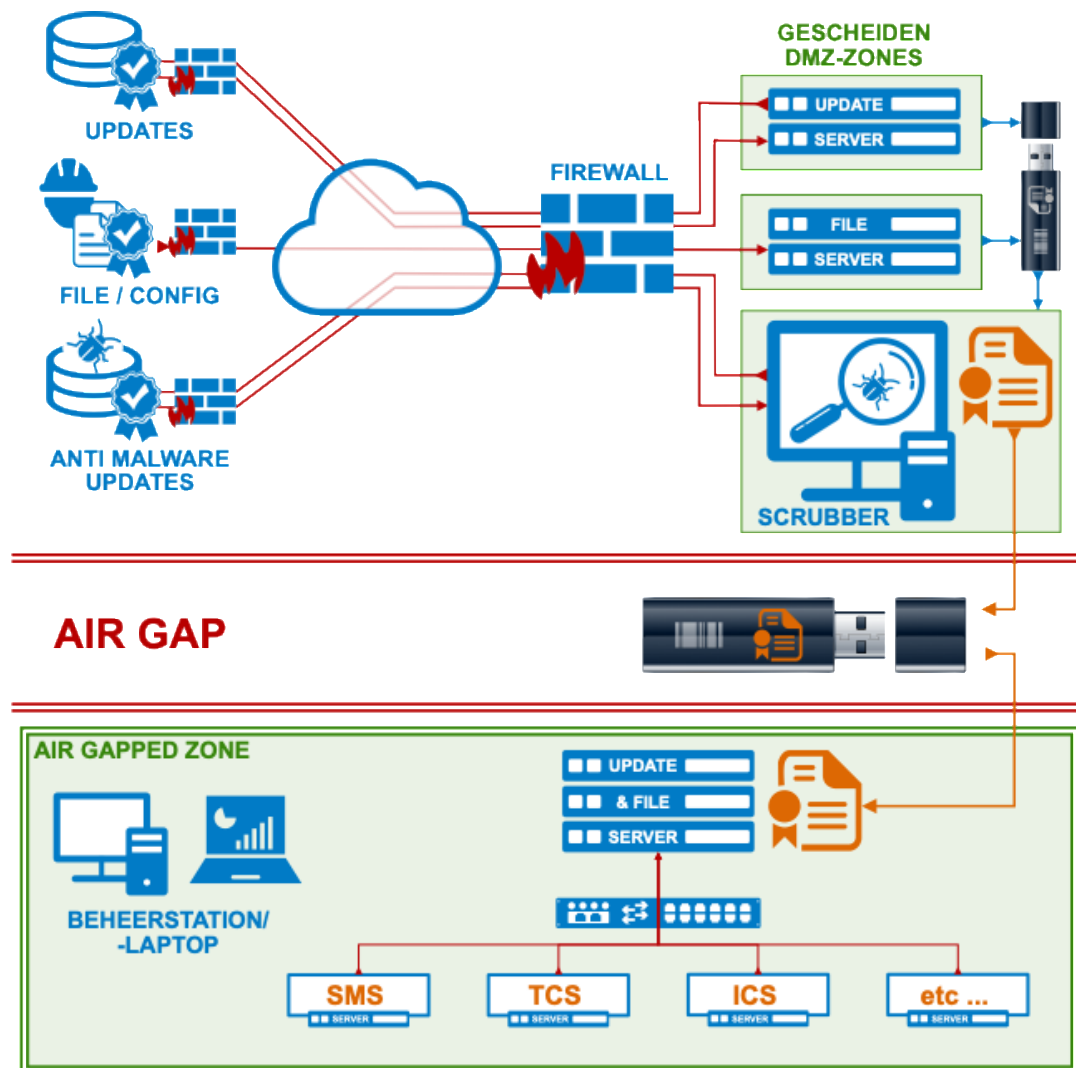
Het online ophalen van updates e.d. vraagt meer planning/afstemming. Daarentegen geeft het ook meer inzicht en controle op het proces.

Als duidelijk is dat een monteur niets mag meenemen, kan hier beter op worden toegezien (duidelijk beleid = duidelijkheid in praktijk bij naleving beleid).
- De **scrubber** moet de datadrager kunnen scannen op digitale dreigingen en gebruikt daarvoor doorgaans meerdere anti-malware programma's om een grotere zekerheid te behalen dan het geval is bij een individuele scanner.
- De Gebruiker stelt een aantal specifieke **datadragers** (bijv. USB-sticks, mobiele SSD harddisks) ter beschikking voor data transfer. De werkwijze is:
 - Data wordt vanuit de DMZ-zones voor updates en/of files op de datadrager gezet.
 - De datadrager wordt aangeboden aan de scrubber.
 - Indien de scrubber digitale dreigingen signaleert, wordt deze gerapporteerd. Uiteraard dienen dan de nodige correctieve acties te worden genomen voor de omgeving en conform security incidentmanagement procedures te worden afgehandeld.
 - Indien géén digitale dreigingen zijn geconstateerd, worden bestanden versleuteld op de datadrager.
 - De server in de air gapped zone dient vooraf van bepaalde software voorzien te zijn, zodat deze uitsluitend de aangewezen datadragers accepteert en uitsluitend toegang krijgt tot de versleutelde bestanden (andere bestanden kunnen niet overgezet worden).
- In het ontwerp van de Vastgoed Gebonden Systemen in de air gapped zone dient rekening gehouden te worden met deze werkwijze en te voorzien worden in:
 - Servers waarop de gescrubde bestanden geplaatst kunnen worden.
 - Voldoende beheerstations/-laptops, zodat het meenemen van beheerlaptops door monteurs niet meer nodig is.

De gedachte van dit ontwerp is dat het schaalbaar toegepast moet kunnen worden, dus voor meerdere (type van) Vastgoed Gebonden Systemen.



VOORBEELD Visuele illustratieve weergave



Figuur 1: Visuele weergave ontwerp



Bijlage E : Specificatie Rapportage VGS

Specificatie Rapportage contractoverleg

Prestaties en gebruik

- Gebruiksrapportage (Zie 7.4 Health Monitoring).
 - Inzicht in prestaties en gebruik
 - Trends en verschillen analyse
 - Alert rapportage

Incidenten

- Status en historie security incidenten, kwetsbaarheden en meldingen

Risico's

- Status Verbeterplannen.
- Wijzigingen in risicodossier

Specificatie Jaarrapportage (op basis van de jaarlijkse inspectie)

Assets

- Actueel overzicht systemen en netwerken;
- Invulling rechten en rollen ter review/accordering management.
- Actuele status compliance aan de door Opdrachtgever geselecteerde CSR eisen. Implementatie-document / (CSP review) – hoog risico-compliant

Risico's

- Actueel risicodossier
- Toezicht op naleving van door Opdrachtgever geselecteerde CSR eisen.
- Actuele status van de risico's en de Verbeterplannen.
 - Welke verbeterpunten zijn uitgevoerd.
 - Welke punten uit de jaarlijkse inspectie worden in de Verbeterplannen opgenomen voor het komende jaar.

Leveranciers

- Actueel Contractregister m.b.t. leveranciersketen(s).
- Actueel *Register vakbekwaamheid leveranciersketen* met daarin de (beschikbare) bewijsstukken voor de ingezette medewerkers van:
 - Vakbekwaamheid voor de betreffende discipline.
 - Het voldoen aan geheimhouding- en screeningsvereisten.
- Beheersing cybersecurity met betrekking tot leveranciersketen (kwalificaties en vaardigheden bedrijven en medewerkers).
- Afhankelijkheden, afspraken en alternatieven in de leveranciersketen in verband met leveringszekerheid.



Bijlage F : Do's en don'ts acceptabel gebruik

Stel instructies op medewerkers omtrent de juiste omgang met en het correct gebruik van Vastgoed Gebonden Systemen. Hierin komen in elk geval de volgende zaken aan bod:

- Het doel en belang van de verschillende systemen
- Het eigenaarschap van de verschillende systemen, en de verdeling van verantwoordelijkheden.
- Monitoring van zaken als netwerkverkeer, persoonsgegevens en/of vertrouwelijke informatie, verwerking van gegevens, handelingen van beheerders.
- Handelingen die zijn toegestaan, zoals bediening systemen, registratie meldingen, etc.
- Handelingen die niet zijn toegestaan, zoals het opladen van een mobiele telefoon via USB, een USB-stick koppelen, browsen naar bepaalde websites, downloaden van illegale content, installeren software, fotograferen vertrouwelijke gebieden/apparatuur.
- Verwacht gedrag zoals omgang met wachtwoorden, in- en uitloggen, correcte omgang met persoonsgegevens en vertrouwelijke informatie, begeleiding van (externe) onderhoudspartijen..
- Onacceptabel gedrag zoals negeren van alarmmeldingen, bewuste foutieve invoer in systemen en het lekken van persoonsgegevens en/of vertrouwelijke informatie.
- Het melden van incidenten via de door Opdrachtgever aangegeven kanalen.



Bijlage G : CMDB

Een *Configuratie Management Database* (CMDB) biedt een compleet overzicht van de verschillende systemen en hun configuraties in een organisatie. Per Vastgoed Gebonden Systeem zijn de volgende zaken geregistreerd:

- VGS type (bijv. Beveiliging)
- VGS naam (bijv. Toegangscontrole)
- Systeemeigenaar
- Beheerpartij
- Leveranciersnaam
- Merknaam/productlijn
- Hardware/onderdeel/component
 - Fabrikantnaam
 - Componentnaam
 - Component type (bijv. server, bedienpaneel, PLC)
 - Korte omschrijving
 - Type/versie
 - Serienummer
 - MAC Address
- Locatie
 - Gebouw
 - Etage
 - Ruimte
 - Rack/kast nummer
 - Rack/kast hoogte
- Software gegevens
 - Applicatiesoftware/Firmware
 - Versie Applicatiesoftware/Firmware
 - Virtualisatie platforms (hypervisor)
 - Versie Hypervisor
 - Besturingssysteem
 - Versie Besturingssysteem
- Identificatie gegevens
 - Host Name
 - DHCP of vast IP?
 - IP-adres
 - Subnetmask
 - Veldbus adres
- Connectiviteit
 - Mogelijkheden:
 - Fysiek (bijv. UTP, ISB-C, serieel)
 - Draadloos (bijv. Bluetooth low energie, NFC, WiFi 6E, Lora)
 - Externe toegang (bijv. VPN, 5G)
 - Actieve connectiviteit (niet hard- of softwarematig uitgeschakeld)
 - Fysiek (bijv. UTP, ISB-C, serieel)
 - Draadloos (bijv. Bluetooth low energie, NFC, WiFi 6E, Lora)
 - Externe toegang (bijv. VPN, 5G)
- Koppelingen met andere systemen



- Lifecycle-data
 - Aanschafdatum
 - Installatiedatum
 - Technische levensduur
 - *End-of-support* (EOS) datum
 - *End-of-life* (EOL) datum
- Audit gegevens
 - Systeem Classificatie: Beschikbaarheid, Integriteit en Vertrouwelijkheid
 - Laatste Inspectie / Audit (Datum)
 - CSR versie van toepassing
 - CSP versie
 - CSP datum laatste review
- Risico gegevens
 - Goedkeuring van Opdrachtgever voor gebruik of toepassing
 - Gerelateerde risicoregistratie(s)
 - Gerelateerde risicoacceptatie + verbeterplan
- Opmerkingen

Dit is een uitgave van het Rijksvastgoedbedrijf

27-7-2026

postbus.rvb.cybersecurityVGS@rijksoverheid.nl

www.rijksvastgoedbedrijf.nl