GVB Cyber Security Principes

1 Samenvatting

In dit document worden de GVB Cyber Security Architectuur Principes beschreven waaraan de onderneming zich moet houden. Dit is een op beveiliging gericht addendum bij de standaard GVB Enterprise principes.

let op Het bron document is bewust in de Engelse taal geschreven om ervoor te zorgen dat het gebruikt kan worden door interne en externe partijen/partners, waarvan sommige geen moedertaalsprekers van het Nederlands zijn. Dit document is een geautomatiseerde vertaling hiervan en er bestaat de mogelijkheid dat sommige vertalingen moeilijker te volgen zijn. In deze gevallen kan er teruggegrepen te worden naar het originele engelse bron document.

2 Versie Geschiedenis

Datum	Versie	Opmerkingen	Gerecenseerd door
14-7-2023	0.1	Eerste ontwerp op basis van sjablonen van The Open Group & ISF SoGP	
30-8-2023	0.2	Geüpdatet concept	Daniël Wunderink Daniel van Dorssen
31-8-2023	0.3	Verwerkte beoordelingscommentaren Daniel W.	Jan Nanne de Jong Cybersecurity-team
8-8-2023	0.4	Verwerkte beoordelingscommentaren Enterprise Architecture & Cybersecurity Team	Ontwerp Raad Albert Fisch
18-9-2023	0.5	Verwerkte commentaren Design Board & Albert Fisch	
27-11-2023	0.9	Versie ter goedkeuring voor IAB, CISO	IAB, CISO
29-10-2023	1.0	Versie goedgekeurd door GAB	GAB

3 Eigenaarschap

Enterprise architectuur is eigenaar van de security principes, waarin expliciete goedkeuring van de CISO noodzakelijk is.

GVB Cyber Security Principes

4 Inhoud

1 Samenvatting....1
2 Versie Geschiedenis....1
3 Eigenaarschap....1
4 Inhoud....2
5 Doel....3
6 Principe relaties....4
7 Principes-sjabloon (richtlijnen)....5
8 Toepasselijkheid....6
9 Overkoepelende beveiligingsprincipes....7
9.1 Overzicht....7
9.2 Gedetailleerde beschrijving per principe....7
10 Verwijzingen....13

5 Doel

Principes zijn algemene regels en richtlijnen, bedoeld om duurzaam te zijn en zelden te worden gewijzigd, die de manier waarop een organisatie haar missie vervult, informeren en ondersteunen.

Principes kunnen op hun beurt slechts één element zijn in een gestructureerd geheel van ideeën die gezamenlijk de organisatie definiëren en sturen, van waarden tot acties en resultaten.

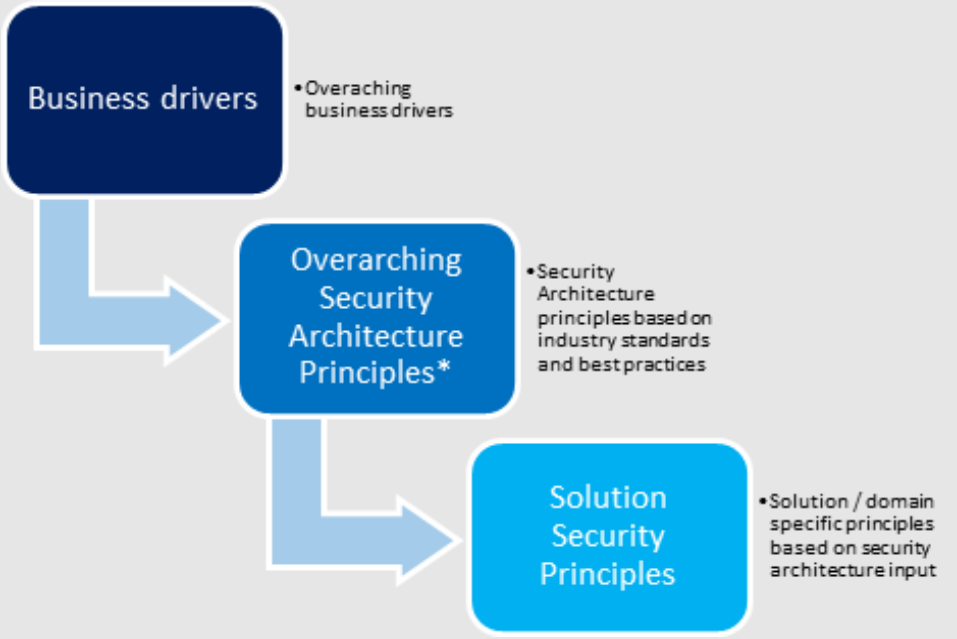
Principes van beveiligingsarchitectuur (ook wel ontwerpprincipes genoemd) zijn fundamenteel voor beveiliging, omdat ze erop gericht zijn om alle GVB-middelen (bijv. Mensen, gegevens en systemen, materiaal, kapitaal, ..) te allen tijde veilig zijn en moeten worden nageleefd bij de ontwikkeling en het gebruik van een beveiligingsarchitectuur, bij het beoordelen en goedkeuren van IT-projecten en bij het uitvoeren van beveiligingscontroles.

6 Principe relaties

De beveiligingsprincipes zijn afgeleid van de business drivers en industriestandaarden en best practices.

We definiëren een reeks overkoepelende beveiligingsprincipes die van hoog niveau zijn en op alle platforms en services moeten worden gebruikt.

Per domein/gebied zullen specifieke oplossingsbeveiligingsprincipes worden ontwikkeld wanneer er behoefte is aan verdere detaillering in richtlijnen:



7 Principes-sjabloon (richtlijnen)

Elk beginsel volgt de volgende richtlijnen:

- De naam moet zowel de essentie van de regel vertegenwoordigen als gemakkelijk te onthouden zijn.
- Specifieke technologieplatforms mogen niet worden genoemd in de naam of verklaring van een beginsel.
- Vermijd dubbelzinnige woorden in de naam en verklaring zoals: "ondersteunen", "openen", "overwegen" en het woord "vermijden" zelf.
- Wees voorzichtig met "manage(ment)", en zoek naar onnodige bijvoeglijke naamwoorden en bijwoorden (fluff).

<ID>	**<Naam van het principe>**
Verklaring	De verklaring moet de fundamentele regel beknopt en ondubbelzinnig overbrengen. Voor het grootste deel zijn de principeverklaringen voor het beheren van informatie van de ene organisatie tot de andere vergelijkbaar. Het is van essentieel belang dat de beginselverklaring ondubbelzinnig is.
Reden	De grondgedachte moet de zakelijke voordelen benadrukken van het naleven van het principe, met behulp van zakelijke terminologie. Wijs op de gelijkenis tussen informatie- en technologieprincipes en de principes die de bedrijfsvoering beheersen. Beschrijf ook de relatie met andere principes, en de intenties met betrekking tot een evenwichtige interpretatie. Beschrijf situaties waarin het ene beginsel voorrang zou krijgen of meer gewicht zou krijgen dan het andere bij het nemen van een beslissing.
Gevolgen	De implicaties moeten de nadruk leggen op de vereisten, zowel voor de business als voor IT, voor het uitvoeren van het principe - in termen van middelen, kosten en activiteiten/taken. Het zal vaak duidelijk zijn dat de huidige systemen, normen of praktijken bij goedkeuring niet in overeenstemming zijn met het principe. De gevolgen voor het bedrijf en de gevolgen van de vaststelling van een beginsel moeten duidelijk worden aangegeven. De lezer dient gemakkelijk het antwoord te kunnen vinden op: "Welke invloed heeft dit op mij?" Het is belangrijk om de impact niet te simplificeren, te bagatelliseren of te beoordelen. Sommige van de implicaties zullen alleen worden geïdentificeerd als potentiële effecten en kunnen speculatief zijn in plaats van volledig geanalyseerd.

8 Toepasselijkheid

Naam	Voorrang van de beginselen
Verklaring	Deze cyber security principes zijn van toepassing op alle organisaties binnen de onderneming.
Reden	De enige manier waarop we besluitvormers een consistent en meetbaar niveau van informatie over de kwaliteit van de beveiliging kunnen bieden, is als alle organisaties zich aan de principes houden.
Gevolgen	Zonder dit principe zouden uitsluitingen, vriendjespolitiek en inconsistentie het beheer van informatie snel ondermijnen. Initiatieven op het gebied van informatiebeheer zullen pas van start gaan als zij zijn onderzocht op naleving van de beginselen. Een conflict met een principe wordt opgelost door het kader van het initiatief te wijzigen.

9 Overkoepelende beveiligingsprincipes

9.1 Overzicht

Id	*Principe*
P-CS-OA-01	**Cyber Security ondersteunt de missie van de organisatie**
P-CS-OA-02	**Veilig door ontwerp (Secure by Design)**
P-CS-OA-03	**Verdediging in de diepte (Defense in Depth)**
P-CS-OA-04	**Standaard beveiligd (Secure by Default)**
P-CS-OA-05	**Minste privileges (Least Privilege)**
P-CS-OA-06	**Standaard weigeren (Default Deny)**
P-CS-OA-07	**Faal veilig (Fail Secure)**
P-CS-OA-08	**Veilig in implementatie (Safe in Implementation)**
P-CS-OA-09	**Bruikbaarheid en beheerbaarheid (Useability & Manageability)**
P-CS-OA-10	**Nooit vertrouwen, altijd verifiëren (Never Trust, Always Verify)**
P-CS-OA-11	**Ga uit van een inbreuk (Assume Breach)**

9.2 Gedetailleerde beschrijving per principe

Id	**P-CS-OA-01**
Naam	**Cyber Security ondersteunt de missie van de organisatie**
Verklaring	Cyber Security heeft als doel om de organisatie te helpen haar missie veilig uit te voeren. Het doel van computerbeveiliging is het beschermen van de waardevolle middelen van een organisatie, zoals informatie, hardware en software.
Reden	Door de selectie en toepassing van passende waarborgen draagt beveiliging bij aan de missie van de organisatie door de bescherming van haar fysieke en financiële middelen, reputatie, rechtspositie, medewerkers, klanten (reizigers) en andere materiële en immateriële activa en zou GVB beter in staat moeten zijn om winst te maken en de dienstverlening aan haar klanten te verbeteren. Veiligheid van de operaties is het hoogste doel.

Gevolgen	-Implementeer goed gekozen beveiligingsregels en -procedures om belangrijke activa te beschermen en de algemene missie van de organisatie te ondersteunen. *Voorbeeld: Lever centrale, gebruiksvriendelijke beveiligingsdiensten die als commodity kunnen worden gebruikt* -Implementeer alleen beveiligingscontroles waar ze nodig zijn op basis van het risico dat dit vormt voor de missie. *Voorbeeld: Baseer de vereiste beveiligingscontroles voor een service op de uitkomst van de BIA+-beoordeling*

Id	**P-CS-OA-02**
Naam	**Veilig door ontwerp**
Verklaring	Beveiliging moet vanaf de basis in het systeem worden ingebouwd - het beveiligingsdenken wordt opgenomen als onderdeel van het ontwerpproces.
Reden	Beschouw de beveiligingsvereisten van een applicatie of systeem als onderdeel van de algemene vereisten, om zichzelf en de informatie die het verwerkt te beschermen en om aanvallen af te weren.
Gevolgen	-Ontwerp beveiliging als een geïntegreerd onderdeel van de systeemarchitectuur gedurende de hele levenscyclus van het systeem (ontwerpen-bouwen-uitvoeren-wijzigen-buiten gebruik stellen) *Voorbeeld: Beveiligingsgericht personeel opnemen in de architectuur, ontwerpen en uitvoeren op basis van best practices uit de branche, zoals OWASP voor webtoepassingen* -Beveiligingsmechanismen moeten alle lagen van de architectuur omvatten en moeten schaalbaar zijn. Alle oplossingen, op maat of commercieel, moeten worden getest op veiligheid. *Voorbeeld: Pentesting en code-analyse van applicaties tijdens de levenscyclus*

Id	**P-CS-OA-03**
Naam	**Verdediging in de diepte**
Verklaring	Vertrouw niet op één (type) verdedigingsmechanisme
Reden	het gebruik van meerdere lagen van verschillende soorten bescherming) om te voorkomen dat u afhankelijk bent van één type of methode van beveiligingscontrole, als één controle faalt, is alles verloren
Gevolgen	-Implementeer meerdere verdedigingsmechanismen; *Voorbeeld: implementeer een firewall en authenticatie en autorisatie op een applicatie. Wanneer de firewall faalt, vertrouwt de applicatie nog steeds op authenticatie en autorisatie om deze veilig te houden.* -Documenteer de verschillende beschermingslagen. -Als een beveiligingsdienst uitvalt, moet het beveiligingssysteem nog steeds bestand zijn tegen bedreigingen. -Compartimenteren en werken met veilige grenzen voor informatiestromen. *Voorbeeld: Voor gegevensoverdrachten buiten een begrensde context moet het gebruik van het HIP-platform nodig zijn*

Getal	**P-CS-OA-04**
Naam	**Standaard beveiligd**
Verklaring	De standaardconfiguratie van de software is zo veilig mogelijk.
Reden	vooraf geselecteerde opties instellen om het niveau van inherente kwetsbaarheid te beperken en alleen noodzakelijke services en functies beschikbaar te stellen
Gevolgen	Implementeer verharding op basis van aanbevelingen van de industrie en leveranciers. *Voorbeeld: Verhardingsinstellingen toepassen die worden beschreven in CIS-benchmarks op componentniveau*

Id	**P-CS-OA-05**
Naam	**Minste privileges**
Verklaring	Alleen de minimaal vereiste bevoegdheden mogen worden verleend aan een gebruiker of een proces voor toegang tot een resource op het moment dat dit vereist is.
Reden	Meer toegang verleend dan strikt noodzakelijk is om haar taken uit te voeren, kan leiden tot ongeoorloofde toegang tot gegevens en systemen.
Gevolgen	-Wijs het minimaal mogelijke aantal machtigingen toe dat nodig is om een functionele rol uit te oefenen; *Voorbeeld: Cdie aangeeft wie systeembeveiligingsfuncties mag in- of uitschakelen of de bevoegdheden van gebruikers of programma's mag wijzigen. Best practice suggereert dat het beter is om meerdere beheerders te hebben met beperkte toegang tot beveiligingsbronnen in plaats van één persoon met "supergebruikers"-machtigingen* - Machtigingen beheren door ze te groeperen en/of toe te wijzen op basis van bepaalde gebruikersparameters; *Voorbeeld: gebruik een set vereiste machtigingen die nodig zijn voor een functionele rol in een "rollengroep" of gebruik attributen om automatisch machtigingen te verlenen aan geautoriseerde functies* - Implementeer just-in-time-mechanismen waarmee tijdelijke getimede toegang kan worden verleend *Voorbeeld: Maak gebruik van EntraID Privileged Identity Management om rollen toe te wijzen die voor een bepaalde tijd kunnen worden geactiveerd voordat ze automatisch verlopen.*

Id	**P-CS-OA-06**
Naam	**Standaard weigeren**
Verklaring	Standaard de toegang tot informatie en systemen ontzeggen
Reden	De standaardinstelling voor een beveiligingscontrole moet zijn om toegang tot een resource te weigeren en een configuratie te vereisen om specifiek toegang te verlenen om ongeoorloofde toegang te voorkomen

Gevolgen	-Authenticatie afdwingen en expliciet alleen geldige autorisaties toestaan voordat toegang wordt verleend tot bronnen of gegevens; *Voorbeeld: Maak regels voor voorwaardelijke toegang die sterke authenticatie vereisen op alle gepubliceerde applicaties van GVB EntraID en blokkeer standaard expliciet alle andere voorwaarden* *Voorbeeld 2: -Bij het instellen van "firewalls" moet de startsituatie een weigeringsregel zijn en bovendien kunnen specifieke toelatingsregels worden toegevoegd wanneer dat nodig is*
Obstakels	-Niet alle resources ondersteunen authenticatie en autorisatie op resourceniveau *Mogelijke beperking: In dit scenario moeten de toepassingen gesegmenteerd zijn in het netwerk en alleen toegankelijk zijn via een toepassingsproxy die de verificatie afhandelt*

Id	**P-CS-OA-07**
Naam	**Fail Secure**
Verklaring	Als een beveiligingscontrole faalt, moet deze een status van toegang weigeren handhaven
Reden	In het geval van een systeemstoring is de informatie niet toegankelijk voor onbevoegden, blijft deze beschikbaar voor bevoegde personen en kan er niet mee worden geknoeid of gewijzigd
Gevolgen	-ontwerp uw beveiligingsmechanisme zo dat een fout hetzelfde uitvoeringspad volgt als het niet toestaan van de bewerking (zie ook Least Privilege) *Voorbeeld: beveiligingsmethoden zoals isGeautoriseerd(), isGeverifieerd() en validate() moeten allemaal false retourneren als er een uitzondering is tijdens de verwerking. (voor meer informatie zie https://owasp.org/www-community/Fail_securely)*

Id	**P-CS-OA-08**
Naam	**Veilig in implementatie**
Verklaring	Beveiligings- en privacy-elementen worden goed begrepen en beheerd tijdens het implementatieproces.
Reden	Om ervoor te zorgen dat de veiligheid en integriteit van ontwikkelde applicaties niet in het gedrang komen tijdens de implementatie.
Gevolgen	-Produceren van schone en onderhoudbare code; -Beveilig uw ontwikkelomgeving; -Bescherm uw coderepository; -Beveilig de build- en implementatiepijplijn; -Test voortdurend uw beveiliging; -Plan voor beveiligingsfouten

Id	**P-CS-OA-09**
Naam	**Bruikbaarheid en beheerbaarheid**
Verklaring	Beveiligingscontroles mogen gebruikers niet belemmeren bij het uitvoeren van hun werk of moeilijk te beheren zijn

Reden	Beveiliging is bedoeld om het bedrijf in staat te stellen zijn doelen veilig te bereiken. Wanneer beveiligingscontroles omslachtig zijn om te gebruiken, zal dit het bedrijf belemmeren in plaats van helpen. De controles zullen ofwel niet worden geaccepteerd of omzeild, wat het doel van de controle tenietdoet.
Gevolgen	-Ontwikkel bedieningselementen die gemakkelijk te gebruiken of (meestal) onzichtbaar zijn voor de gebruiker tijdens normale operaties; -Dwing maatregelen af die passend zijn bij de risico classificatie , implementeer alleen de controls die nodig zijn en niet meer welke passen binnen de kaders van het GVB cyber security beleid; *Voorbeeld: Integreer en gebruik de controls als onderdeel van GVB managed services zoals de managed workplace of managed server omgeving zoals monitoring, endpoint detection & response* -Voeg alleen bedieningselementen toe waar en wanneer ze nodig zijn *Voorbeeld: Vereis geen gegevensversleuteling voor openbaar geclassificeerde gegevens*

Id	**P-CS-OA-10**
Naam	**Nooit vertrouwen, altijd verifiëren**
Verklaring	Vertrouw niet impliciet op locaties, netwerken, systemen of mensen.
Reden	Het beveiligingsmodel dat impliciet vertrouwen impliceert op basis van een netwerk, locatie enz. is gebrekkig. Aanvallers bevinden zich binnen het netwerk en hebben in dit model bijna onbeperkte toegang tot bronnen. (Zie Inbreuk veronderstellen)
Gevolgen	-Authenticeer altijd op het niveau van de individuele resource; -Controleer de autorisatie altijd op het niveau van de individuele resource;
Obstakels	-Niet alle resources ondersteunen authenticatie en autorisatie op resourceniveau *Mitigatie: In dit scenario moeten de toepassingen gesegmenteerd zijn in het netwerk en alleen toegankelijk zijn via een toepassingsproxy die de verificatie afhandelt*

Id	**P-CS-OA-011**
Naam	**Ga uit van een inbreuk**
Verklaring	Werk in de veronderstelling dat GVB of haar partners al zijn gehackt.
Reden	Elk systeem, account of persoon kan op elk moment een potentiële aanvalsvector zijn. Met zo'n groot aanvalsoppervlak moet je ervan uitgaan dat aanvallers ten minste één vector zullen doorbreken als ze dat nog niet hebben gedaan.

Gevolgen	- Identificeren, registreren en labelen van de meest kritische data/systemen; *Voorbeeld: Registreer alle systemen met classificatie in een centrale CMDB en tag Azure-resources op basis van bijvoorbeeld het belang ervan* -Minimaliseer de straal van de explosie (impact tussen systemen) door zijwaartse beweging te voorkomen; *Voorbeeld: Scheidingvan toegang op identiteits- en netwerkniveau tot de meest kritische data/systemen* - Ikvervul de minste privileges voor toegang tot middelen en activa zoals gegevens, systemen, applicaties enz.; - Vaststellen van mogelijkheden voor het detecteren en reageren op bedreigingen; *Voorbeeld: Implementeer Endpoint Detection & Response (EDR) op alle ondersteunde operationele systemen en ontwikkel draaiboeken voor responsacties na een compromis* - Bescherm de identiteit; *Voorbeeld: Maak gebruik van sterke multi-factor authenticatie en controleer op afwijkingen in gebruikersgedrag met behulp van User Entity Behavioural Analytics (UEBA)"* - Vertrouw nooit, verifieer altijd (zie bijbehorend principe) - Anticipeer op menselijke fouten *Voorbeeld: Stel dat een gebruiker op een vislink kan klikken of een onveilig wachtwoord kan instellen en bewustmakingscampagnes kan opzetten om gebruikers voor te lichten en mitigerende controles kan opnemen, zoals een sterk wachtwoordbeleid / wachtwoordloze authenticatie en anti-fishing controls.*

10 Verwijzingen

Bron	Referentie
ISF-norm voor goede praktijken	ISF_Standard_of Good_Practice_for_Information_Security_2022_Excel.xlsx
Zero Trust-principes van Microsoft	https://www.microsoft.com/en-us/security/business/zero-trust#:~:text=Use%20least%2Dprivilege%20access%3A%20limit,detect%20threats%2C%20and%20improve%20defenses .
CISA Security by Design & Security by Default principebenadering	https://www.cisa.gov/sites/default/files/2023-04/principles_approaches_for_security-by-design-default_508_0.pdf
NIST 800-53 – Beveiligings- en privacycontroles voor informatiesystemen en -organisaties	https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
OWASP	https://owasp.org/