Ministerie van Volksgezondheid,
Welzijn en Sport

CIBG BEVEILIGINGSOVEREENKOMST - [LEVERANCIER]

Beveiligingsafspraken en criteria – versie 1.2

1. Inleiding

1.1. Aanleiding

Dit document beschrijft de informatiebeveiligingsafspraken en de daaraan gerelateerde criteria tussen CIBG en [LEVERANCIER] in relatie tot de door CIBG afgenomen diensten: Hosting omgeving [APPLICATIE] CIBG.

1.2. Opzet

De opzet is gebaseerd op de ISO27002:2017, de Code voor Informatiebeveiliging en daarmee op de Baseline Informatiebeveiliging Rijksdienst (BIR:2017).

1.3. Scope

Dit document is onderdeel van de overeenkomst tussen CIBG en [LEVERANCIER] en heeft betrekking op alle hosting diensten die door [LEVERANCIER] aan CIBG in dit kader wordt geleverd met betrekking tot de hosting omgeving [APPLICATIE].

Dit document beschrijft enkel de afspraken en criteria rondom het beheer van diensten, de volgende onderwerpen zijn daarmee expliciet buiten scope:

- Beveiligingseisen voor de software ontwikkeling methodiek (Secure Software Development Lifecycle);
- Het veilig gebruik van voorzieningen en diensten.

1.4. Onderhoud

Dit document wordt minimaal een keer per jaar door beide partijen gereviewd en waar nodig bijgesteld.

1.5. Leeswijzer

Voor onderstreepte woorden is achterin een begrippenlijst opgenomen die de binnen dit document gehanteerde definitie beschrijft.

Gearceerde woorden zijn Engelse vaktermen waarvan de betekenis in de context van informatiebeveiliging bekend wordt verondersteld.

In de paragraaf *Afspraken en criteria* is voor [LEVERANCIER] met (A) aangegeven welke zaken additioneel zijn ten opzichte van de standaard contractafspraken.

1.6. Versie historie

Aanpassing door	Aanpassing	Datum	Versie
Jeroen Kulk	Eerste concept versie	27 maart 2014	0.1
Jeroen Kulk	Tweede concept versie	4 mei 2014	0.2
Loek Zonnenberg	Derde concept versie	5 mei 2014	0.3
Frits Jonkbloed	Geen aanpassing	6 mei 2014	0.4
Loek Zonnenberg	Resultaat nadere afstemming doorgevoerd	15 dec. 2015	0.5
Loek Zonnenberg	Finale afstemming i.s.m. Ton de Bruijn doorgevoerd	7 jan. 2016	1.0
Loek Zonnenberg	Rapportage verbeteringen	16 febr. 2016	1.1
Loek Zonnenberg	Actualiseren hoofdstuk 5	23 okt. 2017	1.2

2. Uitgangspunten

De volgende uitgangspunten dienen als basis voor een goede en veilige samenwerking en dienstenlevering met betrekking tot Hosting omgeving [APPLICATIE] CIBG.

Gezamenlijke verantwoordelijkheid
Informatiebeveiliging is voor CIBG een van de pijlers voor het leveren van betrouwbare diensten en producten. Er is daarbij sprake van een gezamenlijke verantwoordelijkheid voor CIBG en haar dienstverleners.

De definitie van wat veilig is en in hoe de gewenste veiligheid op werkbare en kostenefficiënte wijze tot stand moet komen zal door betrokken partijen in onderlinge afstemming moeten worden bepaald. Informatieveiligheid kan alleen verwezenlijkt worden wanneer eenieder zijn eigen verantwoordelijkheden kent. Daarnaast zet CIBG bij samenwerking in op wederzijdse ondersteuning bij het invullen van de respectievelijke eigen verantwoordelijkheden.

CIBG verwacht van haar [LEVERANCIER]s daarom dat zij niet alleen acteren wanneer hen iets gevraagd wordt, maar ook dat zij de rol van goed huisvaderschap vervullen en adequaat acteren bij dreigende beveiligingsincidenten, falende beveiligingsmaatregelen en proactief inspelen op ontwikkelingen in het dreigingsveld.

Beveiliging als *enabler*
Beveiligingsnormen en maatregelen mogen in de visie van CIBG geen reden zijn om gevraagde functionaliteit zonder meer af te wijzen. CIBG verwacht van haar [LEVERANCIER]s dat zij in een dergelijke situatie met een (technisch) oplossingsvoorstel komt.

Beveiligingsmaatregelen dienen daarnaast bij voorkeur voor de gebruiker zoveel mogelijk transparant te zijn. Het vertrekpunt bij systeemontwerp is dat ze gebruikersgemak en functionaliteit zo min mogelijk frustreren.

Gebruik van standaarden en *best practices*
Als onderdeel van de Rijksoverheid past CIBG de Rijksbrede kaders toe en maakt daarbij zoveel mogelijk gebruik van algemeen geaccepteerde standaarden en *best practices* op het vlak van informatiebeveiliging.

Het verplichte gebruik van deze standaarden geldt niet alleen voor CIBG, maar ook voor haar diensten[LEVERANCIER]s . Deze voor de Rijksoverheid voorgeschreven aanpak draagt bij aan een eenduidige, uniforme benadering van informatiebeveiliging.

Daar waar specifieke afspraken - of CIBG beleid - rondom informatiebeveiligingsonderwerpen ontbreken, worden de algemeen erkende beveiligingsstandaarden en best practices als kaderstellend beschouwd, zowel voor CIBG als haar diensten[LEVERANCIER]s. Deze kaders zijn in het hoofdstuk ‘Wettelijke en CIBG specifieke kaders’ dikgedrukt aangegeven.

3. Afspraken en criteria

3.1. Risicobeoordeling en Risicobehandeling

Opmerking: met (A) is aangegeven welke zaken additioneel zijn ten opzichte van de standaard contractafspraken met [LEVERANCIER].

Risicobeoordeling en risico behandelingen – afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Evalueren van het bij de te leveren dienst behorende actieplan.	P (A)	O

Risicobeoordeling en risico behandelingen - criteria	
Uitvoeren van de evaluatie van het actieplan	1x per half jaar (A)

3.2. Beveiligingsbeleid

Beveiligingsbeleid - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
[LEVERANCIER] tijdig voorzien van laatste versies van de CIBG Beveiligingsnormen en gerelateerd beleid.		P
Opstellen actieplan om beleidsaanpassingen door te kunnen vertalen naar wijzigingen op de dienstverlening.	P (A)	

Beveiligingsbeleid - criteria	
Aanleveren laatste versies	Binnen 30 dagen na vaststelling
Aanleveren bijgewerkt actieplan	Binnen 30 dagen na oplevering

3.3. Organisatie van Informatiebeveiliging

Organisatie van Informatiebeveiliging - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Een deskundig ´*single point of contact*' leveren voor dagelijks Beveiligingsbeheer	P	P

Organisatie van Informatiebeveiliging - criteria	
Doorgeven wijzigingen contactpersonen	14 dagen voorafgaand wijziging

3.3.1. Tactisch Security Overleg

Eén keer in de 3 maanden vindt er tactisch security overleg plaats tussen de security officers van het gehele afnemersgebied en [LEVERANCIER]. Doel van dit overleg is om security gerelateerde onderwerpen met een tactisch karakter te bespreken, zoals:

- De beveiligingsmaatregelen binnen de generieke (ITIL) beheerprocessen,
- De beveiligingsmaatregelen binnen de door [LEVERANCIER] geleverde generieke en gemeenschappelijke IT diensten,
- Vraagstukken en knelpunten ten aanzien van informatiebeveiliging die spelen voor het gehele afnemersgebied,
- Actieplannen voor de verschillende diensten.

3.3.2. Operationeel Security Overleg

Indien één van de verschillende CIBG organisaties het noodzakelijk acht vindt er één keer per maand een operationeel security overleg plaats tussen de operationeel verantwoordelijke beveiligingsfunctionarissen van de desbetreffende CIBG organisatie en [LEVERANCIER].

Doel van dit overleg is om security gerelateerde onderwerpen met een operationeel karakter te bespreken, zoals:

- Afhandeling en analyse van beveiligingsincidenten
- Afstemming en bespreking wijzigingsverzoeken met hoge security impact. Deze changes worden tevens in de Architectectuurboard CIBG besproken waarbinnen security is vertegenwoordigd.
- Afstemming en bespreking uitkomsten pentesten en *vulnerability scans.*
- Afstemming en bespreking *advisories* uitgebracht door het NCSC.

3.4. Beheer van Bedrijfsmiddelen

Beheer van bedrijfsmiddelen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Alle gebruikte diensten en middelen dienen te worden geclassificeerd (WBP) en gerubriceerd (VIRBI) overeenkomstig de processen waar zij ingezet worden of de gegevens die verwerkt worden.	nvt	P
De classificatie/rubricering wordt in de CMDB bijgehouden.	O	P

Beheer van bedrijfsmiddelen - criteria	
Rapportage ontbrekende classificaties en rubriceringen.	nvt
Inzage in CMDB	nvt

3.5. Beveiliging van Personeel

Risicobeoordeling en risico behandelingen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Alle ten behoeve van de aan CIBG te leveren diensten werkzame medewerkers worden op de hoogte gehouden van het CIBG beveiligingsbeleid zover dit noodzakelijk is voor de werkzaamheden.	P	O
Alle ten behoeve van de aan CIBG te leveren diensten werkzame medewerkers dienen te beschikken over de juiste informatiebeveiligingskennis en -kunde die noodzakelijk is voor de werkzaamheden.	P	
Bij ondersteuning van en instructies aan CIBG medewerkers wordt gewezen op de mogelijke risico's en hoe vanuit beveiligingsoptiek op passende wijze om wordt gegaan met diensten en middelen.	P	O
Van alle ten behoeve van de aan CIBG te leveren diensten werkzame medewerkers met mogelijke toegang tot CIBG gegevens heeft [LEVERANCIER] een geheimhoudingsverklaring.	P	

3.6. Fysieke Beveiliging

Fysieke Beveiliging - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Computerruimtes die worden ingezet ten behoeve van de aan CIBG te leveren diensten zijn voorzien van passende maatregelen overeenkomstig de beveiligingseisen van de te leveren diensten. Voor zover deze ruimtes zich bevinden binnen gebouwen van CIBG zijn hierop tevens de binnen de Rijksdienst daarvoor opgestelde normenkaders (zoals het NkBR) van toepassing. De datacenters van [LEVERANCIER] hebben het beveiligingsniveau Tier-3 volgens de TIA-942 norm en voldoen aan ISO27001.	P	
Er zijn procedures om, indien noodzakelijk, CIBG personeel of namens CIBG handelende derden op gepaste wijze toegang te verlenen tot de ten behoeve van CIBG in gebruik zijnde computerruimtes.	P	O

3.7. Beheer van Communicatie- en Bedieningsprocessen

Beheer van communicatie- en bedieningsprocessen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Iedere dienst heeft een beschreven (technische / operationele) beveiligingsbaseline. Invulling [LEVERANCIER]: Naast de generieke Security Baseline die onderdeel is van het ISMS (zie par. 2. Uitgangspunten hierboven), zijn er Technische Baselines per technisch (OS) platform, zoals verschillende Windows, Unix en Linux versies en Netwerk.	P	O
De implementatie van deze baselines wordt regulier gecontroleerd.	P	
De beoordeling van aanpassingen en/of afwijking van de generieke beveiligingsbaseline (ISMS) wordt besproken in het Tactisch Security Overleg..	P	P
Voor iedere standaard change is de impact bepaald en is een standaard *roll-back* of *fall-back* scenario aanwezig.	P	
Voor iedere niet gestandaardiseerde wijziging op de dienstverlening wordt een impact analyse, inclusief beleidstoets, uitgevoerd en wordt een een *roll-back* / *fall-back* scenario opgesteld.	P	
Voor noodzakelijke niet standaard wijzigingen waarvan de uitkomst van deze beleidstoets negatief is, wordt via de Exceptieprocedure naar een tijdelijke oplossing gezocht waarvan de risico's voor beide partijen aanvaardbaar zijn.	P (A)	P
Alle geaccordeerde gedogen worden bij voorkeur opgenomen in het DAP (Dossier Afspraken en Procedures) of in een Exceptieregister geregistreerd, inclusief eind datum, en worden actief gemonitord.	P	
De *signatures*, *patterns* en *blacklists* ten behoeve van de technische maatregelen (*anti-malware*, spam filters, content filters, IDS/IPS) dienen up-to-date te zijn.	P	
Bij signalering van zgn. *zero day exploits* wordt door [LEVERANCIER] de classificatie (op basis van de *cvss* score) bepaald.	P	
Bij *zero day exploits* met mogelijke hoge impact zal [LEVERANCIER] in overleg met CIBG de verdere aanpak bepalen.	P	O
Kritische handelingen en gebeurtenissen op een systeem die relevant zijn voor de monitoring van de informatiebeveiligingsmaatregelen worden gelogd.	P	
Loginformatie wordt (afhankelijk van de mogelijkheden) in doorzoekbaar formaat of door middel van een systeem met passende zoekfunctionaliteit op aanvraag beschikbaar worden gesteld aan door CIBG aan te wijzen functionarissen.	P (A)	

Beheer van communicatie- en bedieningsprocessen – criteria	
Controle en rapportage implementatie Generieke Beveiligingsbaseline (ISMS)	1 x per jaar (ISO27001)
Rapportage mislukte / teruggedraaide changes	1x per maand
Maximale gedoogduur tot herbeoordeling	1 jaar
Rapportage nieuwe, bestaande en verstreken gedogen	1x per maand
Installeren laatste *signatures*, *patterns* en *blacklists*	Binnen 24u (A)
Rapportage status *signatures*, *patterns* en *blacklists*	1x per maand (A)
Rapportage ontbrekende *signatures*, *patterns* en *blacklists*	1x per maand (A)
Classificeren van *zero day exploits*	Binnen 24u
Advies bij *zero day exploit* met mogelijk hoge impact	Binnen 24u
Toegang Loginformatie	Op aanvraag (A)

3.8. Toegangsbeveiliging

Toegangsbeveiliging - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Alle gebruikers en beheeraccounts die door [LEVERANCIER] worden gebruikt dienen als zodanig te zijn gelabeld.	P	
Alle service accounts dienen als zodanig te zijn gelabeld.	P	O
Alle gebruikersaccounts die niet expliciet op naam zijn gesteld dienen als zodanig te zijn gelabeld.	P	O
Alle accounts met verhoogde privileges dienen als zodanig te zijn gelabeld.	P	
Alle ongebruikte accounts dienen te worden geblokkeerd.	P	
Er wordt actief gemonitord op conflicterende rollen binnen de beheeromgeving	P	

Toegangsbeveiliging - criteria	
Rapportage CIBG Service accounts	1x per kwartaal (A)
Rapportage CIBG niet op naam gestelde accounts	1x per kwartaal (A)
Rapportage CIBG *privileged* accounts	1x per kwartaal (A)
Blokkade ongebruikte accounts na	180 dagen
Verwijdering ongebruikte accounts na	240 dagen

3.9. Verwerving, Ontwikkeling en Onderhoud van Informatiesystemen

Verwerving, Ontwikkeling en Onderhoud van informatiesystemen - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Alle in gebruik zijnde informatiesystemen en software dienen, voor in gebruik name, te worden gecertificeerd.	O	P
Een inventaris (CMDB) van alle in gebruik zijnde informatiesystemen en software, bijbehorende versiegegevens, de applicaties die daarop draaien en de onderlinge samenhang, wordt centraal bijgehouden.	P (A)	O
Vulnerability scans wordt regelmatig uitgevoerd ter verificatie van de patchlevels en het opsporen van overige bekende kwetsbaarheden.	P	
Alle in gebruik zijnde informatiesystemen en software dienen tijdig te zijn voorzien van *security patches*[1].	P	
[LEVERANCIER] rapporteert over de in de omgeving aanwezige, door haar beheerde software die niet *up-to-date* is (aantallen, datum release, huidige versie, geïnstalleerde versie).	P	
[LEVERANCIER] rapporteert tijdig over naderende *end-of-life* status van de door haar beheerde informatiesystemen en software.	P	
CIBG draagt zorg voor tijdige compatibiliteit van haar (bedrijfs)applicatie ten behoeve van patchlevels en de vervanging van *end-of-life* informatiesystemen en software.		P

[1] Bij waardering van patches wordt gebruikt gemaakt van het oordeel van de [LEVERANCIER] of vindt waardering plaats op basis van de CVSS score van de gerelateerde kwetsbaarheden,

Verwerving, Ontwikkeling en Onderhoud van informatiesystemen - criteria	
Installeren High Priority Patches	Binnen 1 week na release
Installeren Medium en Low Priority Patches	Bij een eerst volgende onderhoudsmoment maar niet later dan een half jaar na release.
Rapportage *vulnerability scans*	1x per maand (A)
Rapportage Patchstatus	1x per maand
Rapportage ontbrekende Patches en verouderde software.	1 x per maand

3.10. Beheer van Informatiebeveiligingsincidenten

Beheer van Informatiebeveiligingsincidenten - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Er is een generiek draaiboek voor incidenten en calamiteiten binnen de dienstverlening.	P	
Er zijn draaiboeken beschikbaar voor een aantal specifieke incidenten binnen de dienstverlening.	P	
Gesignaleerde (dreigende) kritieke incidenten (*major incidents*) worden aan het informatiebeveiligingsaanspreekpunt van beide partijen gemeld. Indien deze buiten kantoortijden plaatsvinden is een calamiteitenprocedure aanwezig	P	P
Na ieder major incident wordt een analyse uitgevoerd van het incident en waar nodig een verbetervoorstel (actieplan) gedaan.	P	
Bij incidenten waarbij mogelijk sprake is van aantasting van integriteit of vertrouwelijkheid van CIBG gegevens zal [LEVERANCIER] op aanvraag medewerking verlenen door gegevens uit de systemen van CIBG ter beschikking te stellen, rekening houdend met wettelijke eisen.	O	P (A)

Beheer van Informatiebeveiligingsincidenten - criteria	
Beschikbare draaiboeken	▪ (onbekende) Malware en virus uitbraak ▪ Spam run (inbound, specifiek gericht op CIBG) ▪ Spam run (outbound, CIBG als verzender) ▪ Denial-of-Service Attacks (A) ▪ Gerichte Hack aanval ▪ Website *defacement*
Melding (dreigend) incident	Volgens P1 procedure (Incidentmanagement)
Rapportage Beveiligingsincidenten	1x per maand
Verbetervoorstel n.a.v. (P1) Incident	Binnen 1 maand

3.11. Bedrijfscontinuïteitsbeheer

Bedrijfscontinuïteitsbeheer - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
Voor iedere dienst dient een continuïteitsplan te zijn opgesteld waarin rekening wordt gehouden met de blijvende werking van de juiste beveiligingsmaatregelen.	P (A)	O
Voor de specifieke technische beveiligingsmaatregelen dient een continuïteitsplan te zijn waarbij de *mean-time-to-recovery* tot een minimum is beperkt.	P (A)	
De continuïteitsplannen dienen regelmatig te worden getest en onderhouden.	P	O

Bedrijfscontinuïteitsbeheer - criteria	
Continuïteitsplannen voor technische Maatregelen en ondersteunende voorzieningen	▪ Identity & access voorzieningen ▪ SIEM (A) ▪ IDS/IPS (A) ▪ Reverse Proxy ▪ Web Application Firewall Interne Firewalls ▪ Network devices

Frequentie van testen	1x per jaar
Rapportage continuïteitstesten	1x per jaar (A)

3.12. Naleving

Naleving - afspraken		
Rollen / Verantwoordelijkheden (P=Primair, O= Ondersteunend)	[LEVERANCIER]	CIBG
[LEVERANCIER] draagt er zorg voor dat de door haar aan CIBG geleverde diensten aantoonbaar voldoen aan de met CIBG gemaakte afspraken.	P	O
[LEVERANCIER] verantwoordt zich over de opzet, bestaan en werking van de aan de dienst gerelateerde beveiligingsmaatregelen aan CIBG middels *assurance* verklaring (ISAE3404 en Third Party Mededeling) die door een derde partij, op basis van marktconforme, door CIBG geaccepteerde standaarden is opgesteld.	P (A)	O
Medewerking en toegang tot noodzakelijk informatie en informatie systemen verlenen ten behoeve van (onaangekondigde) audits en controles van beveiligingsmaatregelen.	P	P
Bij beëindiging of wijziging van de dienstverlening worden op verzoek van CIBG alle gegevens waarvoor CIBG verantwoordelijk is en/of waarvan CIBG eigenaar is tijdig en in bruikbaar formaat overgedragen aan CIBG.	P (A)	
Er worden regulier pentesten op de geleverde diensten en onderliggende voorzieningen uitgevoerd om de technische beveiligingsmaatregelen te controleren.	O	P

Naleving - criteria	
Assurance verklaring / Third party mededeling	1x per jaar
Overdracht gegevens bij beëindiging dienst	Binnen 1 maand
Pentest rapportage	nvt

4. Begrippenlijst

Actieplan	Dienst specifiek beveiligingsplan wat een overzicht geeft van de geïmplementeerde maatregelen en de te ondernemen acties en planning beschrijft om ontbrekende of falende beveiligingsmaatregelen te implementeren of verbeteren. die noodzakelijk zijn om aan de bij de dienst behorende beschikbaarheids-, integriteits- en vertrouwelijkheidseisen te kunnen blijven voldoen Deze acties zijn afkomstig uit de verschillende beheer- (incident management, *vulnerability management*) en audit rapportages.
Beveiligingsmaatregelen	Alle maatregelen van technische, organisatorische en/of procedurele aard die worden ingezet om mogelijke beveiligingsrisico's te voorkomen of te beperken.
Zero-day-exploit	*Zero-day-exploits* (software die daadwerkelijk via een gat in de beveiliging gebruik maakt van het uitvoeren van een aanval) worden gebruikt of gedeeld door aanvallers vóór de ontwikkelaars van de doelsoftware iets afweten van de kwetsbaarheid.
Website defacement	Het ongewild van buitenaf aanpassen van webpagina's door ongeautoriseerde (hackers)
Beveiligingsbaseline	Beschrijving van de toepassing van de dienst (als onderdeel van een High Level Design, Fuctioneel/Technisch ontwerp, Solution architecture of ander ontwerp document) en de bijbehorende, als veilig beschouwde, technische basisconfiguratie van de dienst en/of de bouwstenen (componenten) waaruit de dienst is opgebouwd.
risico acceptatie	Met een risico acceptatie accepteert de afnemer de risico's voor een oplossing die afwijkt van de vastgestelde baselines en afspraken – voor deze gedoogsituatie vervalt de SLA en ondersteund de [LEVERANCIER] op basis van *best effort*. Technisch gezien verdient het aanbeveling dergelijke gedoogsituaties zoveel mogelijk te isoleren van de standaard productieomgeving.
kritiek incident	Er is sprake van een kritiek of *major* incident wanneer een incident een grote of directe impact heeft, dient de afnemer geïnformeerd te worden zodat deze op passende wijze kan acteren. Er is dan sprake van een kritiek Incident. • Beschikbaarheid: – Incident waarbij de in de SLA vastgelegde norm voor een dienst wordt overschreden; – Incident waarbij meerdere diensten gelijktijdig zijn geraakt; • Integriteit: – Incident waarbij kritische of vertrouwelijke data ongecontroleerd is aangepast; • Vertrouwelijkheid: – Incident waarbij ongeautoriseerde toegang tot kritische of vertrouwelijke systemen heeft plaatsgevonden;
Kritische handelingen	Een handeling waarbij sprake is van toegang tot vertrouwelijke gegevens of die de integriteit van de gegevens kunnen aantasten.
CVSS	*Common Vulnerability Scoring System* (http://www.first.org/cvss) – Een scoringssysteem voor het op gestandaardiseerde wijze waarderen van IT kwetsbaarheden.
Priviliged accounts	*Privileged* accounts zijn accounts met mogelijk speciale

	toegangsrechten, waarbij onderscheid gemaakt kan worden in de volgende type accounts: - Algemene beheeraccounts: nodig voor het algehele beheer van een systeem. - Applicatie-, service- en system accounts: Accounts die niet worden gebruikt door een natuurlijk persoon maar door applicaties, services en systemen. - Privileged of power user accounts: accounts die zijn toegekend aan een gebruiker of groep gebruikers die additionele rechten nodig hebben voor het uitvoeren van hun functie.
niet op naam gestelde gebruikersaccounts	Gebruikersaccounts die niet zijn gekoppeld aan een specifieke natuurlijke gebruiker. Bijvoorbeeld test-accounts of opleidingsaccounts. De verantwoordelijkheid voor het gebruik van een dergelijk account wordt voor deze account belegd bij de hiertoe gemandateerde aanvrager (lijnmanager).

5. Wettelijke en CIBG specifieke kaders

[LEVERANCIER] dient steeds de vigerende regelgeving na te leven. Onderstaande regelgeving kan dus worden aangevuld met nieuwe regelgeving en de aangegeven versie dient steeds “de vigerende versie” te zijn. [LEVERANCIER] dient deze derhalve na te leven zoals bedoeld in de toepasselijke overeenkomst met CIBG

Kader	**Organisatie**	**Versie**
Wet Bescherming Persoonsgegevens	Concern	2000
AV-23: Beveiliging van Persoonsgegevens, Achtergrondstudies en verkenningen	Concern	2001
Algemene Verordening Gegevensbescherming	Concern	2018
Beveiligingsvoorschrift Rijksdienst (BVR:2013)	Concern	2013
Het Besluit Voorschrift Informatiebeveiliging Rijksdienst (VIR:2007)	Concern	2007
Het Besluit Voorschrift Informatiebeveiliging Rijksdienst – Bijzondere Informatie (VIRBI:2013)	Concern	2013
Baseline Informatiebeveiliging Rijksdienst (BIR:2017)	Concern	V1.0
Norm voor Informatiebeveiliging (NEN-ISO/IEC 27001:2017)	Concern	2017
Norm voor Informatiebeveiliging (NEN-ISO/IEC 27002:2017)	Concern	2017
Statuut Integrale Beveiliging CIBG	Concern	V1.0
ETSI EN 319 411-1	CIBG	V2.1.1
ETSI EN 319 411-2	CIBG	V2.2.0
EU verordening 910/2014 (EIDAS)	Concern	2014
CEN TS 419261:2015	CIBG	2015
Logius eisen Public Key Infrastructure (PKI) voor de overheid	CIBG	V4.5
Logius Norm ICT-beveiligingsassessments DigiD	CIBG	V2.0
NCSC ICT-beveiligingsrichtlijnen voor webapplicaties - deel 1	Concern	V2.0