SOC Team
Zwarte Woud 2
3524 SJ Utrecht
Telefoon 030 252 3004
Email [redacted]

Checklist Onboarding Applicaties

Eerst controleren, daarna aanschaffen

Definitieve versie: 1.02

Opdrachtgever	[redacted]
Auteur	[redacted]
Kwaliteitszorg	
Rapportnummer	
Classificatie	Intern
Status	Definitief
Datum	26 maart 2021
File Naam	Checklist Onboarding Applicaties

Template versie 0.02

Inhoud

Documentbeheer

Versiebeheer

Versie	Datum	Auteur	Omschrijving verandering	Status
0.01	09-03-2021	[redacted]	Initiële opzet	Concept
0.02	10-03-2021	[redacted]	Beveiligingsmaatregelen	Concept
0.90	10-03-2021	[redacted]	Proces	Concept
1.00	11-03-2021	[redacted]	Finaliseren na accordering	Definitief
1.01	25-03-2021	[redacted]	Verbeteren op basis feedback	Concept
1.02	26-03-2021	[redacted]	Finaliseren na accordering	Definitief

Gecontroleerd door

Versie	Datum	Naam	Functie
0.90	10-03-2021	[redacted]	[redacted]
1.01	26-03-2021	[redacted]	[redacted]

Geautoriseerd door

Versie	Datum	Naam	Functie
1.00	11-03-2021	[redacted]	[redacted]
1.02	26-03-2021	[redacted]	[redacted]

Gerelateerde documenten

Documenttitel	Omschrijving
Algemene Verordening Gegevensbescherming (AVG)	Europese privacy-verordening
Baseline Informatiebeveiliging Overheid (BIO)	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013
NEN 7510 – Informatiebeveiliging in de Zorg	Nederlandse richtlijn, gebaseerd op de internationale standaard ISO/IEC 27001:2013 en specifiek voor de zorgsector

Volgende review en/of herziening, plus accordering (tenzij eerdere update)

Datum	Functie voor bewaking
01-06-2021	[redacted]

1. Inleiding

Met deze checklist wil GGD GHOR borgen dat applicaties die worden aangeschaft passen binnen de infrastructuur van de GGD'en en op een veilige en betrouwbare wijze gegevens verwerken.

1.1. Scope en doelgroep

Deze checklist is van toepassing op alle applicaties die worden aangeschaft ter ondersteuning van de werkzaamheden van GGD GHOR en de GGD'en.

De doelgroep bestaat uit de GGD'en, partners voor de digitale infrastructuur en leveranciers van SaaS-oplossingen, programmatuur en apparatuur.

1.2. Rollen en verantwoordelijkheden

De Chief Information Officer (CIO) van GGD GHOR is verantwoordelijk voor de inhoud van deze checklist.

De inkopende afdelingsmanager is verantwoordelijk voor het invullen van de checklist en deze toe te zenden aan het Security Operating Center (SOC) van GGD GHOR.

Het SOC is verantwoordelijk om de checklist te verifiëren en te interveniëren als blijkt dat een aan te schaffen applicatie leidt tot risico's voor de beschikbaarheid van de dienstverlening, of de integriteit of vertrouwelijkheid van de te verwerken gegevens.

Interventies door het SOC worden gerapporteerd aan de CIO, de Chief Information Security Officer (CISO) en de Functionaris voor de Gegevensbescherming (FG) van GGD GHOR.

1.3. Richtlijn voor het gebruik van de checklist

De checklist bevat een aantal aandachtspunten. Deze zijn niet voor alle toepassingen relevant en, waar nodig, mogen op 'Niet van toepassing' (Nvt) worden gezet. Van belang is dat wordt nagedacht over de betreffende aandachtspunten en weloverwogen wordt vastgesteld of deze wel of niet van toepassing zijn.

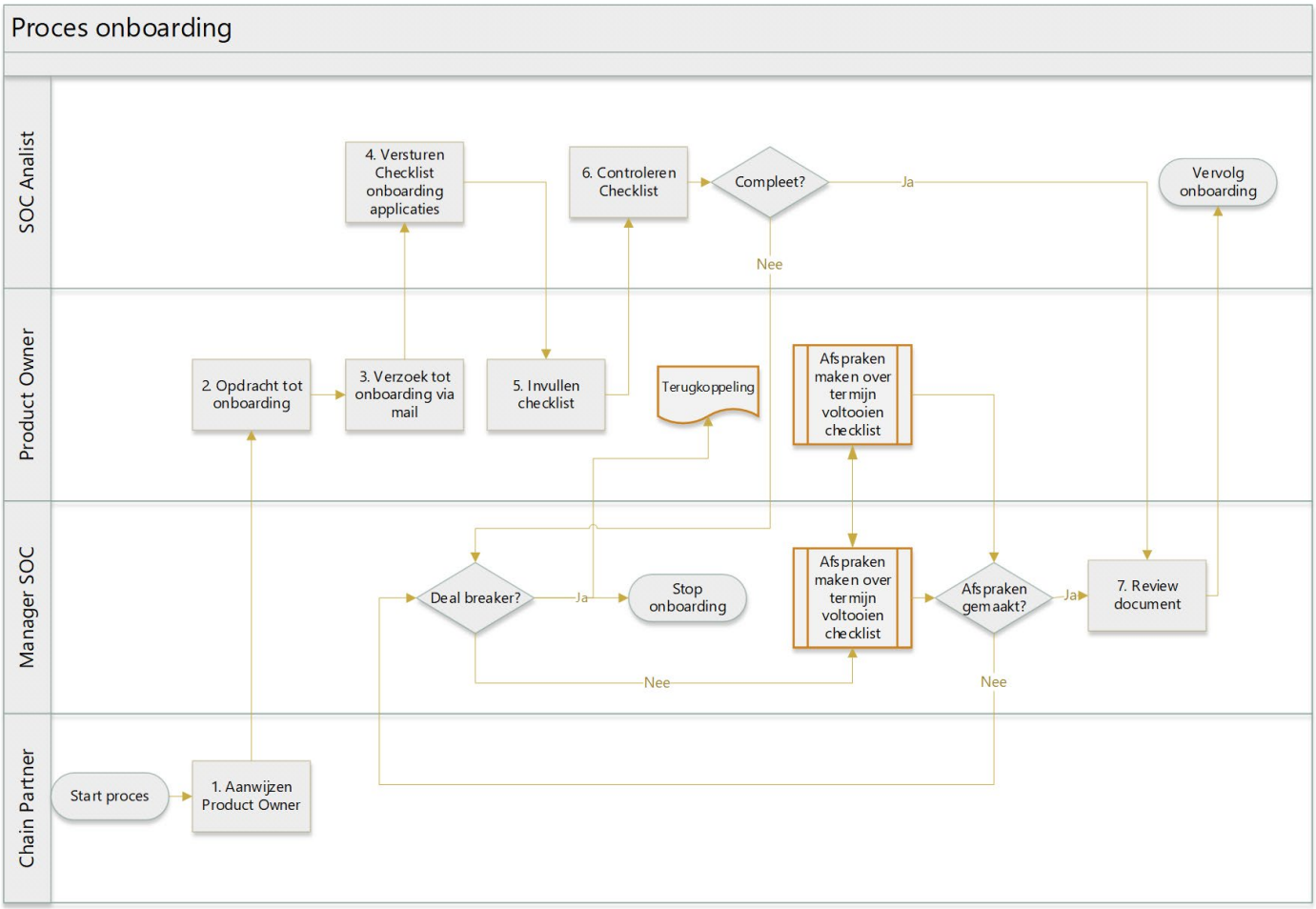
1.4. Review of audit door het SOC

Desgewenst kan het SOC een review of audit uitvoeren op een applicatie. Dit wordt met name geadviseerd voor applicaties die gevoelige persoonsgegevens verwerken of die onderdeel zijn van een essentieel bedrijfsproces bij een GGD.

1.5. Onderhoud van de checklist

Het SOC onderhoudt de checklist en communiceert deze naar de GGD'en.

2. Proces voor controle onboarding



De stappen binnen het proces zijn:

1. **Aanwijzen Product Owner**
   Deze wordt aangewezen door de ketenpartner;

2. **Opdracht tot onboarding**
   De Product Owner besluit dat controle nodig is, gezien een mogelijk risico dat kan worden veroorzaakt door de installatie of het gebruik van de applicatie;

3. **Verzoek tot onboarding via mail**
   De Product Owner licht het SOC in over de voorgenomen aanschaf van de applicatie;

4. **Versturen checklist onboarding applicaties**
   Het SOC stuurt de actuele versie van de checklist aan de Product Owner;

5. **Invullen checklist**
   De Product Owner laat de checklist invullen, bij voorkeur in overleg met de lokale CISO en, indien sprake is van het verwerken van persoonsgegevens, met de lokale Privacy Officer (PO) en/of FG. De ingevulde checklist wordt naar het SOC gestuurd;

6. **Controleren checklist**
   Het SOC controleert de ingevulde checklist op volledigheid en verifieert de risico-inschatting van de Product Owner. Dit kan leiden tot verder overleg, onder andere over aanpassing van de risico-classificatie of over de te treffen mitigerende maatregelen. Dit kan eventueel leiden tot het afwijzen van de applicatie. Als naar de mening van het SOC een getrouw beeld is gevormd van de risico's en risicomitigatie, wordt de review van de ingevulde checklist afgerond;

7. **Review document**
   De Manager SOC neemt het besluit of de onboarding van de applicatie kan worden gecontinu-eerd.

3. Eisen voor applicaties

In de onderstaande tabel is de 'Vlag' bedoeld om het risico van een eventuele afwijking weer te geven, met:

Vlag	Ernst	Toelichting
H	Hoog	Onacceptabel risico voor integere en vertrouwelijke gegevensverwerking.
M	Midden	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor complexe compenserende maatregelen nodig zijn.
L	Laag	Risico voor integere en vertrouwelijke gegevensverwerking, waarvoor eenvoudige compenserende maatregelen nodig zijn.

3.1. Werknemers en applicatiegebruikers

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
1.1	Awareness van gebruikers en beheerders voor integriteit en vertrouwelijkheid bij het gebruik is geborgd					
1.2	De gebruiker ziet een notificatie bij opstarten, waarin staat dat de regels moeten worden gevolgd					
1.3	Procedures voor uitgeven, muteren en innemen van accounts en authenticatiemiddelen, uitgeven en resetten van wachtwoorden etc. zijn ingericht					
1.4	Gebruikers zijn ingelicht dat accounts niet mogen worden gedeeld					
1.5	Use cases voor verdacht en onverdacht gebruik (voor analyse in het SIEM) zijn beschikbaar					
1.6	Monitoren van verdachte en onverdachte activiteiten van de gebruiker is mogelijk					

3.2. Coding en systeemdocumentatie

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
2.1	Een formele standaard wordt gevolgd voor ontwerpdocumentatie					
2.2	Het functioneel ontwerp is beschikbaar					
2.3	Het technisch ontwerp is beschikbaar					
2.4	Het autorisatiebeheer in de applicatie kan worden gekoppeld aan het centrale rollenbeheer					
2.5	Logging en monitoring zijn beschikbaar					
2.6	De schaalbaarheid is geborgd, dus capaciteit kan worden uitgebreid					
2.7	Het uitvoeren van op beveiliging gerichte testsessies is mogelijk					
2.8	Formele standaard documentatie over interface(s) is beschikbaar					
2.9	De koppelingen garanderen volledige en correcte gegevensoverdracht					
2.10	Cryptografie is toegepast op de applicatie en API’s					

3.3. Testen op kwetsbaarheden in de beveiliging

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
3.1	Kwetsbaarheden bij het verzamelen van informatie, zoals het ontdekken van toepassingen, toegangspunten voor toepassingen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.2	Kwetsbaarheden in configuratiebeheer, zoals toegang tot beheerdersinterfaces, SSL-zwakte, XSS-risico en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.3	Autorisatiekwetsbaarheden en authenticatiekwetsbaarheden zoals het opsommen van gebruikers, het doorlopen van paden, het manipuleren van rollen en meer zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.4	Kwetsbaarheden in gegevensvalidatie, zoals SQL / LDAP / SMTP / code-injectie zijn in kaart gebracht en gemitigeerd of formeel geaccepteerd door de risico-eigenaar					
3.5	Penetratietests zijn uitgevoerd en gepland					

3.4. Infrastructuur, back-up en monitoring

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
4.1	De continuïteit van de applicatie is geborgd via redundante voorzieningen					
4.2	Een realtime beveiligingsservice is toegepast					
4.3	Back-ups worden regelmatig of realtime geproduceerd en restore-testen worden regelmatig uitgevoerd					
4.4	Maatregelen zijn getroffen om back-ups te beschermen tegen ransomware, via isolatie en controles					
4.5	Monitoring van blootgestelde services					
4.6	Monitoring van interne diensten					
4.7	Gevoelige omgevingen zijn geïsoleerd op netwerkniveau, door een veilige netwerkarchitectuur met VLAN's					
4.8	De toegang tot interne services en IP-adressen is beheerst					
4.9	OS- en docker-images zijn up-to-date					
4.10	Gezag en toezicht op de Data Base Administrators (DBA's) is ingericht					
4.11	Gebruik van een Ontwikkel, Test, Acceptatie en Productie (OTAP)-straat is geborgd					

3.5. Organisatie

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
5.1	De applicatie past binnen de veiligheidscultuur					
5.2	De applicatie draagt bij aan transparantie over diensten en gegevensverzamelingen					
5.3	De applicatie is niet in strijd met het beleid in-zake openbare veiligheid					
5.4	De applicatie is niet in strijd met de naleving van het organisatiebeleid en wettelijke vereis-ten					
5.5	De applicatie past binnen het beleid voor be-drijfscontinuïteit en noodherstel					

3.6. Dienstverlener

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.1	De uptime in de SLA, die door dienstverlener wordt verstrekt, is geverifieerd					
6.2	Technische ondersteuning is beschikbaar van-uit de dienstverlener					
6.3	De geldigheid van certificaten, zoals ISO 27001, NEN 7510 etc. is geverifieerd					
6.4	Er is geverifieerd dat uitwijk mogelijk is naar een beveiligde uitwijklocatie					
6.5	Er is geverifieerd dat gegevens worden versleu-teld tijdens transport via het interne netwerk					
6.6	Er is geverifieerd dat persoonsgegevens wor-den verwerkt conform de AVG (dit betreft PII – Personal Identifiable Information)					

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
6.7	Er is geverifieerd dat persoonsgegevens alleen binnen de Europese Economische Ruimte (EER) worden opgeslagen en altijd binnen de EER blijven					

3.7. Beheerprocessen

3.7.1. Autorisatiebeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
7.1	Gedocumenteerde procedures voor autorisatiebeheer zijn beschikbaar					
7.2	Het gezamenlijk gebruik van een account is niet toegestaan (dus geen groepsaccounts, altijd individuele accounts)					
7.3	Rollen zijn gebaseerd op aantoonbare functiescheiding					
7.4	Accounts zijn ingedeeld in logisch opgebouwde groepen (zoals Organizational Units – OU's – in de AD), bijvoorbeeld als eindgebruiker, administrator, mailbox, service-account etc.					
7.5	Het afdwingen van een wachtwoordbeleid dat voldoet aan de BIO is ingericht					
7.6	Een adequate lock-out policy ter voorkoming van brute force aanval met raden van wachtwoorden is ingericht					
7.7	2-Factor Authenticatie is toegepast					
7.8	Periodieke controles op accounts ter voorkoming van vervuiling worden uitgevoerd					
7.9	Rapportage over accounts is beschikbaar					

3.7.2. Configuratiebeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
8.1	Configuratie-items zijn geregistreerd in een Configuratie Management Data Base (CMDB), inclusief hun BIV-classificatie					
8.2	Een procedure voor het beheer en onderhoud van de CMDB is ingericht					
8.3	Rapportagefaciliteiten voor de configuratie-items in de CMDB zijn beschikbaar					

3.7.3. Wijzigingenbeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
9.1	De classificatie van wijzigingen is ingericht					
9.2	De registratie en afhandeling van wijzigingen is ingericht					
9.3	De bewaking en tijdige afhandeling van wijzigingen is ingericht					
9.4	De evaluatie van mislukte wijzigingen is ingericht					
9.5	Rapportage over wijzigingen, wel of niet succesvol geïmplementeerd, en tijdigheid is ingericht					

3.7.4. Incident- en probleembeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
10.1	De classificatie voor reguliere incidenten en beveiligingsincidenten is ingericht					
10.2	De registratie- en afhandeling van incidenten en problemen is ingericht					
10.3	De bewaking van tijdige afhandeling van incidenten en problemen is ingericht					
10.4	Incidentevaluatie en -preventie is ingericht					
10.5	Een reactieplan voor beveiligingsincidenten (incident response plan) is opgesteld en actueel					

3.7.5. Beveiligingsbeheer

Nr.	Beveiligingsmaatregel	J	N	Nvt	Vlag	Toelichting
11.1	De fysieke toegangsbeveiliging is ingericht					
11.2	De bescherming tegen phishing is ingericht					
11.3	De bescherming tegen DDoS-aanvallen is ingericht					
11.4	De bescherming tegen ransomware is ingericht					
11.5	Domeinen zijn afgeschermd, waar nodig					
11.6	De bescherming van domeinnamen is ingericht					
11.7	Het gebruik van beveiligde wifi-verbindingen is geborgd					
11.8	Het gebruik van Virtual Private Network (VPN), waar noodzakelijk, is geborgd					
11.9	De Demilitarized Zone (DMZ) is ingericht					
11.10	Intrusion Detection System (IDS) en Intrusion Prevention System (IPS) zijn ingericht					
11.11	De web application firewall en reverse proxy zijn ingericht					

Bijlage A Lijst van afkortingen

Afkorting	Toelichting
AD	Active Directory, Microsoft
API	Application Programming Interface
AVG	Algemene Verordening Gegevensbescherming
BIO	Baseline Informatiebeveiliging Overheid
BIV	Beschikbaarheid, Integriteit en Vertrouwelijkheid
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Data Base
DBA	Data Base Administrator
DMZ	Demilitarized Zone. Dit is een nul-netwerk met een binnen-firewall en een buiten-firewall, om te zorgen voor isolatie tussen netwerken.
DDoS	Distributed Denial of Service
EER	Europese Economische Ruimte
FG	Functionaris voor de Gegevensbescherming
IAM	Identity and Access Management
IDS	Intrusion Detection System
IP	Internet Protocol
IPS	Intrusion Prevention System
LDAP	Lightweight Directory Access Protocol. Het netwerkprotocol dat beschrijft hoe gegevens uit directoryservices moeten worden benaderd.
OS	Operating System
OTAP	Ontwikkel, Test, Acceptatie en Productie
OU	Organizational Units in de AD
PII	Personal Identifiable Information
PO	Privacy Officer
SaaS	Software as a Service. Dit zijn veelal applicaties die via een web-oplossing worden geleverd.
SDLC	Software Development Life Cycle
SIEM	Security Information and Event Management
SLA	Service Level Agreement
SMTP	Simple Mail Transfer Protocol
SOC	Security Operating Center
SQL	Structured Query Language. Dit is een programmeertaal voor toegang tot gegevensbestanden.
SSL	Secure Socket Layer. SSL is verouderd. TLS 1.2 of hoger dient te worden gebruikt.
VLAN	Virtual Local Area Network
VPN	Virtual Private Network. Dit is een versleutelde verbinding over internet.
XSS	Cross Site Scripting