

Checklijst nieuwe leverancier PC (Windows varianten)

Rollen en verantwoordelijkheden leverancier PC

DIENT ICT

Van: Dennis Krijgsman

Aan: MT Dienst ICT

Cc.:

Datum: 16-2-2023

Versie	Datum wijziging	Auteur	Omschrijving	Rol
1.0	06-1-2022	D.P Krijgsman	Eerste goedgekeurde versie	A
1.1	10-5-2022	D.P Krijgsman	Toegevoegd IOT checklijst	A
1.2	4-4-2023	D.P Krijgsman	Laptops toegevoegd	A

Distributielijst

Naam	Rol	Versie 1.1	Versie 1.2	Versie 1.3
WBO	A			
Hans van de Heuvel	C		C	
Niels Weening	C			
Marcel de Kuiper	C			
Wilson Kwartan	C			
Arnoud Jippes	C			
Mark de wilde			R	

Rollen:

Auteur= A

Reviewer = R

Contributor = C

Goedkeurder = G

Inhoud

Inleiding.....	2
Checklijst aansluiten Windows 10 IoT editie	3
Aanvulling op aansluitvoorwaarden voor laptops i.c.m. IOT Windows 10.....	5
Checklijst Windows 10 overige edities (Professional/Enterprise)	7
Aanvulling op aansluitvoorwaarden voor laptops i.c.m. Windows Professional/Enterprise	11
Afspraken, rollen en verantwoordelijkheden.....	13
Ondertekening voor akkoord leverancier/afdeling	15

Inleiding

Definitie leverancier PC/Laptop: Een computer die geleverd wordt door een externe leverancier en die wordt voorzien van applicatie(s) of randapparatuur om (onderzoeks) handelingen uit te voeren. Deze PC/Laptop wordt ondersteund door de externe partij, binnen de kaders die de afdeling met de leverancier heeft afgesproken.

Een leverancier PC/laptop kan worden ingezet wanneer het niet mogelijk is om een Dienst-ICT geleverde PC in te zetten, wat te maken heeft met ondersteuning en certificering die de externe leverancier afdwingt op de leverancier PC configuratie.

De leverancier PC/laptop is een Windows PC configuratie die onderdeel is van een samengesteld systeem, bedoeld voor gebruik in het Amsterdam UMC, waarbij een koppeling met het datanetwerk en Active Directory benodigd is. Bij een samengesteld systeem is sprake van een applicatie met bijbehorende werkplek(ken) die de rol van acquisitie- of dataverwerking station vervullen, die altijd door een externe leverancier wordt geleverd. Om afdelingen en leveranciers bewust te maken van de security beleidskaders omtrent het aansluiten van leverancier PC's of laptops, is in dit document een checklijst verwerkt waaraan de leverancier moet voldoen. Omdat er grote verschillen zijn tussen een [Windows 10 IOT variant\(desktop/laptop\)](#) of [Windows Professional/Enterprise variant\(desktop/laptop\)](#), bestaat dit document uit twee checklijsten met ieder zijn eigen security eisen.

Ondersteuning leverancier PC's door de Dienst-ICT: Ondersteuning van leverancier PC's is beperkt, de producten die Dienst-ICT wel ondersteunt zijn aangegeven in Tabel 1 Ondersteuning op leverancier PC's.

*In het document als leverancier pc wordt benoemd kan dit refereren naar een desktop of laptop hardware.

Ondersteuning	Beschrijving	Ondersteunde Dienst
Anti-Malware	Als de installatie van de anti-malware impact heeft op de functionele werking van de leverancier PC, dan dient de Dienst-ICT hiervoor benaderd te worden.	Dienst-ICT
Shares koppeling op leverancier PC	Hulp bij configuratie van shares op de leverancier PC.	Dienst-ICT
CMDB registratie	De machine en software wordt in de CMDB geregistreerd.	Dienst-ICT

Tabel 1 Ondersteuning op leverancier PC's

Checklijst aansluiten Windows 10 IoT editie

De hoofdaannemer van de klantaanvraag zorgt ervoor dat de onderstaande IOT checklijst wordt ingevuld samen met de leverancier van de PC.

Maatregel	Beschrijving	Verplicht	Verantwoordelijk	Leverancier akkoord? (Ja/Nee) Indien nee, beschrijf waarom niet.
Application control	Er wordt alleen gebruik gemaakt worden van applicaties die vooraf zijn goedgekeurd door het Amsterdam UMC.	Ja	Leverancier	Kies een item.
Windows defender application control (WDAC)	Er wordt alleen gebruik gemaakt van applicaties en drivers die vooraf zijn goedgekeurd door het Amsterdam UMC.	Ja	Leverancier	Kies een item.
Security baseline (GPO)	De security baseline van Microsoft is actief. Inclusief de host base firewall welke least privilege is geconfigureerd.	Ja	Leverancier	Kies een item.
Filtering of blokkade van USB apparatuur	Voor het gebruik van USB apparatuur op de leverancier pc is toestemming nodig van het Amsterdam UMC.	Ja	Leverancier	Kies een item.
Keyboard filter	Het gebruik van toetsen combinaties op de leverancier pc is niet mogelijk.	Nee	Leverancier	Kies een item.
Unified write filter (UWF = kiosk modus)	De leverancier pc staat standaard in read-only modus.	Ja	Leverancier	Kies een item.
Netwerk connectiviteit	Het systeem is voorzien van één netwerkinterface. Bridge functionaliteit tussen meerdere netwerksegmenten is niet toegestaan.	Ja	Leverancier	Kies een item.
Rapid 7 full scan	Bij het plaatsen van de leverancier pc zal er éénmalig met een de vulnerability scanner (Rapid 7) een volledige scan uitgevoerd worden.	Ja	Leverancier	Kies een item.

	Dit om kwetsbaarheden en hardenings niveau inzichtelijk te maken.			
Rapid 7 scheduled vulnerability scan	Het Amsterdam UMC zal maandelijks een front scan uitvoeren met de Rapid 7 tooling.	Ja	Leverancier	Kies een item.
Overige interfaces	Interfaces zoals Wi-Fi, Bluetooth, NFC zijn uitgeschakeld. Uitsluitend in overleg en wanneer de noodzaak wordt aangetoond kan een uitzondering gemaakt worden.	Ja	Aanvrager/leverancier	Kies een item.

Tabel 2 Checklijst aansluitvoorwaarden Windows 10 IoT

Indien er gedeeltelijk of niet voldaan kan worden aan de eisen van de aansluitvoorwaarden, dan moet de casus besproken worden met security architectuur. Als de leverancier akkoord is met de gestelde voorwaarden dan mag het systeem zonder aanvullende securitymaatregelen aangesloten worden op het netwerk.

Aanvulling op aansluitvoorwaarden voor laptops i.c.m. IOT Windows 10

Maatregel	Beschrijving	Verplicht *	Verantwoordelijk	Kan de leverancier aan voldoen?
Plaatsing laptop	De laptop moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met Amsterdam UMC badge met de juiste autorisaties.	Ja	Aanvrager	Kies een item.
Fysiek slot op laptop	Bij de aanschaf van een leveranciers laptop moet ook een 'laptop kabel slot' aangeschaft worden. Bij plaatsing van de laptop wordt het slot ook direct gebruikt.	Ja	Aanvrager	Kies een item.
Wireless internet	Bij voorkeur wordt de leverancier laptop bedraad aangesloten. Als aantoonbaar dit niet mogelijk is, wordt de laptop draadloos verbonden aan een beveiligde WIFI verbinding.	Ja	Aanvrager	Kies een item.

Netwerk USB dongles	Er wordt geen gebruik gemaakt van netwerk dongles.	Ja	Aanvrager	Kies een item.
Data laptop	Data opgeslagen op de laptop moet periodiek verplaatst worden naar interne Amsterdam UMC netwerkshares.	Ja	Aanvrager	Kies een item.

Tabel 3 Extra aansluitvoorwaarden t.b.v. laptops i.c.m. Windows IOT

Checklijst Windows 10 overige edities (Professional/Enterprise)

De hoofdaannemer van de klantaanvraag zorgt ervoor dat de onderstaande checklijst voor professional/Enterprise edities wordt ingevuld samen met de leverancier van de PC.

Maatregel	Beschrijving	Verplicht *	Verantwoordelijk	Kan de leverancier aan voldoen?
Voldoen aan aansluitvoorwaarden	Iedere leverancier PC dient te voldoen aan de op dat moment geldende aansluitvoorwaarden. De leverancier pc voldoet aan de eisen uit de aansluitvoorwaarden. (Link)	Ja	Aanvrager & Leverancier	Kies een item.
OS support	Het geïnstalleerde OS (operatie systeem) moet ondersteund zijn door Microsoft, en gemaakt zijn voor PC's. (Windows 10) Het OS heeft geen end of support of end of life status, tijdens de periode dat de leveranciers pc in gebruik is van het Amsterdam UMC.	Ja	Aanvrager & Leverancier	Kies een item.
Drivers en bios updates	Tijdens de periode dat een leveranciers pc in gebruik is door het Amsterdam UMC. Bevatten de bios en drivers geen kwetsbaarheden.	Ja	Aanvrager & Leverancier	Kies een item.
Software	Software die geïnstalleerd wordt door de leveranciers op een leverancier PC moet bijgewerkt worden door de leverancier. De software loopt nooit meer dan 1 versie achter en security updates worden direct geplaatst.	Ja	Aanvrager & Leverancier	Kies een item.

Active directory	Leverancier PC's worden geplaatst in een leveranciers OU binnen een Amsterdam UMC domein.	Ja	Dienst-ICT	Kies een item.
Maandelijkse Windows Security updates	Maandelijks worden er door de Dienst ICT security updates op de leverancier PC geïnstalleerd.	Ja	Dienst-ICT	Kies een item.
Windows Feature updates	Het Windows operatie systeem voor werkplekken (OS) moet periodiek door de leverancier worden bijgewerkt, zodat het geïnstalleerde OS binnen support van Microsoft blijft (Feature updates/ Windows as a service proces).	Ja	Aanvrager & Leverancier	Kies een item.
Apart netwerk segment	Leverancier PC's worden geplaatst in een apart netwerk segment, niet op hetzelfde netwerk segment van Dienst ICT werkplekken.	Ja	Dienst-ICT	Kies een item.
Security baseline	Elke leverancier-PC die aangesloten worden op het Amsterdam UMC domein, zal worden voorzien van de standaard Microsoft beveiliging-instellingen. (Group policy)	Ja	Dienst-ICT	Kies een item.
Installatie van een antivirus applicatie	Op de leverancier PC wordt door de Dienst ICT een antimalware product geïnstalleerd. Op moment van Schrijven is dit McAfee/Trellix (agent cliënt en ENS software).	Ja	Dienst-ICT	Kies een item.

Uitzonderingsregels antivirus	Voor sommige software is het nodig om scan uitzonderingen te maken, deze worden in overleg met security/CERT toegepast.	Nee (Software kan correct werken met de standaard antivirus configuratie)	Dienst-ICT	Kies een item.
SCCM	Op elke leverancier PC wordt een SCCM agent geïnstalleerd.	Ja	Dienst-ICT	Kies een item.
SCCM rechten	Het SCCM account wordt toegevoegd aan de lokale administrators groep.	Ja	Dienst-ICT	Kies een item.
Rapid 7	De Rapid7 kwetsbaarheden scanner zal geïnstalleerd worden op de leverancier PC. Indien er kwetsbaarheden gevonden worden, zal dit aan de afdeling worden doorgegeven.	Ja	Dienst-ICT	Kies een item.
Remote toegang	Indien er sprake is van remote toegang voor de leverancier, dan moet standaard de remote oplossing van het Amsterdam UMC "Bomgar" gebruikt worden.	Ja	Dienst-ICT	Kies een item.
Plaatsing leverancier PC	De PC moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met Amsterdam UMC badge met de juiste autorisaties.	Ja	Aanvrager	Kies een item.

Het gebruik van accounts i.c.m. default wachtwoorden.	Het gebruik van standaard wachtwoorden en account is niet toegestaan binnen het Amsterdam UMC. Het account en wachtwoord moet uniek zijn voor het Amsterdam UMC.	Ja	Aanvrager/leverancier	Kies een item.
Overige interfaces	Interfaces zoals Wi-Fi, Bluetooth, NFC worden uitgeschakeld wanneer deze niet aantoonbaar noodzakelijk zijn.	Ja	Aanvrager/leverancier	Kies een item.

Tabel 4 Checklijst Windows 10 Professional/Enterprise edities

* De hoofdaannemer bespreekt de leverancier PC met de aanvrager en de leverancier bij het tot stand komen van het inkoopdossier. De afwijkingen van de checklijst zal worden aangegeven bij Dienst-ICT. De Dienst-ICT zal de afwijkingen en mogelijkheden intern bespreken, om ervoor te zorgen dat de leverancier PC wordt aangeschaft en aangesloten op een veilige en functionele manier.

Aanvulling op aansluitvoorwaarden voor laptops i.c.m. Windows Professional/Enterprise

Maatregel	Beschrijving	Verplicht *	Verantwoordelijk	Kan de leverancier aan voldoen?
Plaatsing laptop	De laptop moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met Amsterdam UMC badge met de juiste autorisaties.	Ja	Aanvrager	Kies een item.
Fysiek slot op laptop	Bij de aanschaf van een leveranciers laptop moet ook een 'laptop kabel slot' aangeschaft worden. Bij plaatsing van de laptop wordt het slot ook direct gebruikt.	Ja	Aanvrager	Kies een item.
Wireless internet	Bij voorkeur wordt de leverancier laptop bedraad aangesloten. Als aantoonbaar dit niet mogelijk is, wordt de laptop draadloos verbonden aan een beveiligde WIFI verbinding.	Ja	Aanvrager	Kies een item.

Netwerk dongles	Er wordt geen gebruik gemaakt van netwerk dongles.	Ja	Aanvrager	Kies een item.
Data laptop	Data opgeslagen op de laptop moet periodiek verplaatst worden naar interne Amsterdam UMC netwerkshares.	Ja	Aanvrager	Kies een item.

Tabel 5 Additionele aansluitvoorwaarden t.b.v. laptops i.c.m. Windows Professional/Enterprise

Afspraken, rollen en verantwoordelijkheden

Omdat er verschillende partijen (afdeling, Dienst ICT en leverancier) betrokken zijn bij het aansluiten en ondersteunen van een nieuwe leverancier PC willen we wijzen op de volgende afspraken, rollen en verantwoordelijken omtrent een leverancier PC:

1. Alle maatregelen die benoemd zijn in dit document, gelden voor de gehele levensduur van de werkplek (zolang deze gebruikt wordt en/of aangesloten is).
2. Door het installeren van de Rapid 7 “Kwetsbaarheden” scanner, worden kwetsbaarheden op een leverancier-PC inzichtelijk. Deze kwetsbaarheden worden door het CERT-Team van de Dienst ICT gemonitord en gerapporteerd aan de verantwoordelijke binnen het Amsterdam UMC.
3. De werkplek wordt beheerd door de afdeling en de leverancier (conform de afspraken die tussen deze twee partijen zijn gemaakt over de hardware en software op de werkplek). De betrokken hoofdaannemer binnen de Dienst ICT zal toetsen op de vastlegging van de afspraken tijdens het inkooptraject.
4. Het aannemerschap binnen de Dienst ICT is onderverdeeld in twee rollen (hoofdaannemer en onderaannemer):
 - Hoofdaannemer; De hoofdaannemer is een team binnen applicatiediensten, de leverancier PC is onderdeel van een samengesteld systeem waarbij altijd een applicatie gebruikt wordt.
 - Onderaannemer; De onderaannemer is werkplekdiensten, de leverancier PC is een werkplek die gebruikt wordt bij een samengesteld systeem in de rol van een acquisitie- of dataverwerking station. Werkplekdiensten zal de leverancier PC aansluiten wanneer deze voldoet aan de checklist die in dit document is beschreven.
5. De Dienst ICT stelt zich op als partij die de leverancier PC aansluit, conform de geldende aansluitvoorwaarden en afspraken die van tevoren overeengekomen zijn.
6. De Dienst ICT verleent alleen ondersteuning op de antivirus applicatie.
7. De Dienst ICT is niet verantwoordelijk voor data verlies op de leverancier werkplek of het terughalen van deze data.
8. De leverancier is verantwoordelijk voor het upgraden en bijhouden van een ondersteund operating system(OS). Denk hierbij aan feature updates van o.a. Windows 10/11 (Windows as a service), die op het moment van levering gelden en de levensduur van de leveranciers PC.
9. Als de leverancier geen security updates toelaat door de Dienst ICT, dan is de leverancier zelf verantwoordelijk voor het updaten van de werkplek conform de aansluitvoorwaarden.
10. Als de werkplek intern verhuist is er een meldplicht vanuit de afdeling.
11. Indien er sprake is van een veiligheidswijziging op de werkplek dan heeft de afdeling een meldplicht naar de Dienst ICT (ongeautoriseerd toegang, data verlies etc.). Een uitgebreide uitleg is te vinden in dit document.
12. Tijdens de levensduur van de leverancier PC moet er eerst toestemming gevraagd worden aan de Dienst ICT, als er afgeweken wordt van de voor afgestemde checklist.
13. Indien er sprake is van (patiënten) data verlies of een veiligheidsincident dan is er een meldplicht bij het CERT/Autoriteit persoonsgegevens binnen het Amsterdam UMC.
14. De leverancier PC's worden intern gemonitord door de Rapid 7 kwetsbaarheden scanner. Bevindingen uit deze scanner worden naar afdeling toegestuurd, en het is taak van de afdeling (en leverancier) om hier actie op te ondernemen.
15. De leverancier PC wordt altijd voorzien van een inventarisatie sticker, deze wordt gebruikt voor de registratie in de CMDB (Configuration Management Database).
16. De Windows updates op de leverancier PC worden standaard uitgevoerd op zondagavond. In overleg kan er afgeweken worden van deze dag en tijdstip.
17. Leverancier PC's mogen alleen aangesloten worden in opdracht van de Dienst ICT.

18. Leverancier PC's die niet voldoen aan de overeengekomen voorwaarden en een veiligheidsrisico vormen voor Amsterdam UMC worden van het netwerk afgesloten.

Verklarende woordenlijst

Woord en of begrip	Uitleg
Aansluitvoorwaarden	Er zijn standaard aansluitvoorwaarden voor het Amsterdam UMC netwerk vastgelegd. De punten in deze checklijst zijn extra veiligheidsmaatregelen bovenop deze standaard voorwaarden en zijn van toepassing op leverancier PC's met een Windows computer operatie systeem.
Active directory aansluiting	De leverancier PC wordt aangesloten op het Amsterdam UMC domein. En wordt binnen dit domein in een aparte OU geplaatst genaamd "Leverancier PC". Hierin wordt een onderscheidt gemaakt op divisie en applicatie.
OS support	De geleverde leverancier PC moet ondersteund worden door Microsoft, en voorzien van een OS die bedoeld is voor computers.
Security updates	Maandelijkse veiligheidsupdates die door Microsoft worden uitgebracht moeten binnen 2 weken geïnstalleerd zijn op de leveranciers PC.
Feature updates	Het geïnstalleerde operatie systeem moet ondersteund blijven door Microsoft, dit kan betekenen dat de leverancier de machine periodiek van "Builds" moet voorzien. Hierdoor kan de leverancier pc blijvend voorzien worden van security updates.
Apart netwerk segment	De leverancier pc wordt in een apart netwerk segment geplaatst, gescheiden van de reguliere Dienst ICT beheerde werkplekken.
Antivirus	In tijd van schrijven wordt standaard McAfee erop geïnstalleerd met een standaard configuratie (instellingen en taken zoals full scan wekelijks).
Uitzonderingen antivirus	Om de applicatie beter te laten functioneren is het soms nodig om mappen of bestanden uit te zonderen van scans. De leverancier moet dit van tevoren aanleveren.
Security baseline	Dit is een set van standaard veiligheidsmaatregelen gedefinieerd door Microsoft die doormiddel van group policy's (beleidsinstellingen) wordt geactiveerd tijdens het plaatsen van de werkplek in het Amsterdam UMC domein. Voor elke build is een andere versie. Je kan de instellingen hier vinden.
SCCM	SCCM of Microsoft endpoint configuration manager agent wordt geïnstalleerd om de machine te voorzien van updates en tools (McAfee Rapid 7)
Rapid 7	Deze tool controleert periodiek of de leverancier PC kwetsbaarheden bevat. Denk aan achterlopen van Windows updates.

Ondertekening voor akkoord leverancier/afdeling

Tekenen akkoord afdeling

Naam:

Handtekening:

Datum:

Tekenen akkoord leverancier

Naam:

Handtekening:

Datum:

Tekenen akkoord hoofdaannemer Dienst ICT

Naam:

Afdeling:

Handtekening:

Datum:
