

Checklijst nieuwe leverancier pc

Controle document aansluiten nieuwe leveranciers werkplekken

AMSTERDAM UMC DIENST ICT

Auteur: Dienst ICT (Afdeling Werkplekdiensten)

Van: Dienst ICT (interne ICT organisatie Amsterdam UMC)
Aan: Externe leveranciers en afdelingen binnen Amsterdam UMC
Cc.:
Versie: 1.4
Datum: 04-03-2025

Inhoudsopgave

Inleiding	3
Checklijst aansluiten Windows 10/Windows 11 IoT Enterprise LTSC	4
Aanvulling op aansluitvoorwaarden voor laptops i.c.m. aansluiten Windows 10/Windows 11 IoT enterprise LTSC	8
Checklijst Windows 10/11 (Professional/Enterprise) LTSC.....	9
Aanvulling op aansluitvoorwaarden voor leverancier laptops i.c.m. checklijst Windows 10/11 (Professional/Enterprise) LTSC.....	14
Afspraken, rollen en verantwoordelijkheden	16
Verklarende woordenlijst	18
Meest gestelde vragen	19
Bijlage voor extra notities	21
Ondertekening akkoord door leverancier.....	22
Ondertekening akkoord door afdeling *	22

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('s) of laptop(s) wordt beheerd door de externe partij, binnen de kaders die de afdeling en Dienst ICT 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. Een voorbeeld hiervan is dat de geleverde PC is opgenomen als onderdeel in het medisch CE-certificaat.

De leverancier PC/laptop is een Windows PC-configuratie die onderdeel is van een samengesteld systeem, bedoeld voor gebruik binnen Amsterdam UMC. Waarbij een koppeling met het datanetwerk en/of 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 vervult, die altijd door een externe leverancier wordt geleverd. Om afdelingen en leveranciers bewust te maken van de security beleidskaders bij 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 (alleen LTSC)/11 IOT variant(desktop/laptop) of Windows Professional/Enterprise variant (desktop/laptop), bestaat dit document uit twee checklijsten met ieder zijn eigen security eisen. De meest gestelde vragen over dit document, vind je onderaan dit document.

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.

Ondersteuning	Beschrijving	Ondersteunde Dienst
Microsoft Defender van Amsterdam UMC	Als de installatie van de Amsterdam UMC beheerde defender impact heeft op de functionele werking van de leverancier PC, dan dient de Dienst-ICT hiervoor benaderd te worden. De lokaal geïnstalleerde Defender moet netwerk toegang krijgen, om defender updates te kunnen verwerken.	Dienst-ICT
Shares koppeling op leverancier PC	Hulp bij configuratie van shares op de leverancier PC.	Dienst-ICT
Rapid 7 kwetsbaarheden scanner	Als de installatie van de kwetsbaarheden scanner, mogelijk impact heeft op de functionele werking van de leverancier PC, dan dient de Dienst-ICT hiervoor benaderd te worden.	Dienst-ICT

CMDB registratie	De volgende items worden registreert in de CMDB: • PC hardware • Software • Eigenaar van PC en • Naam leverancier software	Dienst-ICT
Software updates	Hulp bij het verbinden van de leverancier PC via Internet voor het ophalen van software updates (bv met Microsoft).	Dienst-ICT

Tabel 1 Ondersteuning leverancier PC's

Checklijst aansluiten Windows 10/Windows 11 IoT Enterprise LTSC

De hoofdaannemer (bij de Dienst ICT) van het demand zorgt ervoor dat de onderstaande checklijst voor Windows IoT wordt ingevuld samen met stakeholders: Leverancier van de PC en betrokken afdeling. **Zorg ervoor dat je de juiste checklijst invult. Voor meer informatie, ga naar hoofdstuk: [Meest gestelde vragen](#).**

Maatregel	Beschrijving	Verplicht	Verantwoordelijke	Gaat de leverancier akkoord met de voorwaarden? (Ja/Nee) Als Nee, beschrijf waarom niet en met voorgestelde alternatieven.
Voldoen aan aansluitvoorwaarden	Iedere leverancier PC dient te voldoen aan de op dat moment geldende aansluitvoorwaarden die opgesteld is door de Dienst ICT. De leverancier PC voldoet aan de eisen uit de aansluitvoorwaarden (Interne Link). Het document waar de link naar verwijst is opvraagbaar.	Ja	Leverancier	

Feature application control	Application control is een onderdeel van Windows IoT. Dit onderdeel moet standaard <u>aan</u> staan, zodat alleen goedgekeurde applicaties gestart kunnen worden.	Ja	Leverancier	
Windows defender application control (WDAC)	Er wordt alleen gebruik gemaakt van applicaties en drivers die vooraf zijn goedgekeurd door Amsterdam UMC.	Ja	Leverancier	
Security baseline (GPO)	De security baseline van Microsoft is ingericht volgens het minste privileges principe.	Ja	Leverancier	
Filtering of blokkade van USB apparatuur	Voor het gebruik van USB apparatuur op de leverancier PC is toestemming nodig van Amsterdam UMC.	Ja	Leverancier	
Unified write filter (UWF = kiosk modus)	De leverancier PC staat standaard in read-only modus. Wijzigingen op het systeem worden niet bewaard als de machine herstart.	Ja	Leverancier	
Netwerk connectiviteit	Het systeem is voorzien van één netwerkinterface. Bridge functionaliteit en routing tussen meerdere netwerksegmenten is niet toegestaan.	Ja	Leverancier	
Rapid 7 agent scan	De geleverde leverancier PC staat een kwetsbaarheidsscan op de PC toe om het beveiligingsniveau te beoordelen en op zoek	Ja	Leverancier	

	te gaan naar kwetsbaarheden. De scan wordt d.m.v. een geïnstalleerde agent uitgevoerd, en de resultaten hiervan worden gedeeld met de leverancier die wordt verzocht om actie te ondernemen om eventuele gedetecteerde kwetsbaarheden te verhelpen. Als er gegronde redenen zijn dat dit niet mogelijk is. Kan er een agentless scan uitgevoerd worden.			
Rapid 7 Periodieke scan	Amsterdam UMC mag periodiek scans uitvoeren op het apparaat om kwetsbaarheden op te sporen. Deze scan is niet-verifiërend (zonder inloggen op het systeem) en heeft een laag profiel (lage intensiteit) wat betreft kwetsbaarheid scans. Deze scan heeft minimale invloed op de functionaliteit van het systeem. De resultaten van deze scan worden gedeeld met de betreffende beheer afdeling en met het ICT security team van Amsterdam UMC.	Ja	Leverancier	
De PC configuratie is gehardend en volgt security “best practices van STIG,CIS of de leverancier”. Dit betekent o.a.:	Het gebruik van standaard wachtwoorden en accounts is niet toegestaan binnen het Amsterdam UMC. Het	Ja	Leverancier	

Leveranciers pc checklijst

- Unieke wachtwoorden. - Alleen noodzakelijk services/protocollen actief. - De software geïnstalleerd is altijd up to date.	account en wachtwoord moet uniek zijn voor het Amsterdam UMC.			
Overige interfaces	Interfaces zoals Wi-Fi, Bluetooth, NFC zijn uitgeschakeld. Als er toch gebruik gemaakt moet worden van deze eerder genoemde interfaces moet dit in overleg met Dienst ICT.	Ja	Leverancier	

Tabel 2 Checklijst aansluitvoorwaarden Windows 10/11 IoT

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

Aanvulling op aansluitvoorwaarden voor laptops i.c.m. aansluiten Windows 10/Windows 11 IoT enterprise LTSC

Maatregel	Beschrijving	Verplicht*	Verantwoordelijk	Gaat de leverancier akkoord met de voorwaarden? (Ja/Nee) Als Nee, beschrijf waarom niet en met voorgestelde alternatieven.
Plaatsing laptop	De laptop moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met een Amsterdam UMC badge en met de juiste autorisaties.	Ja	Aanvrager	
Fysiek slot op de laptop	Bij de aanschaf van een leverancier laptop moet ook een 'laptop kabel slot' aangeschaft worden. Bij plaatsing van de laptop wordt het slot ook direct gebruikt.	Ja	Aanvrager	
Wireless internet laptop (uitzondering)	Standaard wordt de leverancier laptop met een UTP kabel aangesloten. Als de leverancier kan aantonen, na overleg met Amsterdam UMC ICT dat dit niet mogelijk is, wordt er gekeken naar een maatwerk oplossing.	Ja	Leverancier	
USB ethernet aansluiting	Er mag geen gebruik gemaakt worden van USB ethernet aansluitingen.	Ja	Leverancier	
Data back-up op laptop	Data back-up op een leveranciers laptop wordt niet gefaciliteerd.	Ja	Aanvrager	

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

Checklijst Windows 10/11 (Professional/Enterprise) LTSC

De hoofdaannemer (Dienst ICT) van de demand zorgt ervoor dat de onderstaande checklijst voor professional/Enterprise edities wordt ingevuld samen met de leverancier van de PC. **Zorg ervoor dat je de juiste checklijst invult voor meer informatie, ga naar hoofdstuk: [Meest gestelde vragen](#).**

Maatregel	Beschrijving	Verplicht *	Verantwoordelijk	Gaat de leverancier akkoord met de voorwaarden? (Ja/Nee) Als Nee, beschrijf waarom niet en met voorgestelde alternatieven.
Voldoen aan aansluitvoorwaarden	Iedere leverancier PC dient te voldoen aan de op dat moment geldende aansluitvoorwaarden die opgesteld is door de Dienst ICT. De leverancier PC voldoet aan de eisen uit de aansluitvoorwaarden (Interne Link). Het document waar de link naar verwijst is opvraagbaar.	Ja	Leverancier	
OS support	Het geïnstalleerde operatie systeem moet ondersteund zijn door Microsoft, en gemaakt zijn voor Pc's. Het OS heeft geen end of support of end of life status, tijdens de periode dat de leverancier PC in gebruik is van Amsterdam UMC. Daarom moeten de geleverde Pc's voorzien zijn van extended support. (Windows versie 10 mag	Ja	Leverancier	

	alleen nog maar geleverd worden met LTSC editie).			
Drivers en bios updates	Tijdens de periode dat een leverancier PC in gebruik is door het Amsterdam UMC bevatten de bios en drivers geen kwetsbaarheden.	Ja	Leverancier	
Software	Software die geïnstalleerd wordt door de leverancier op een leverancier PC moet bijgewerkt worden door de leverancier. De software loopt nooit meer dan 1 versie achter en security updates worden direct geïnstalleerd.	Ja	Leverancier	
Active directory	Leverancier PC's worden geplaatst in een leveranciers OU binnen een Amsterdam UMC domein.	Ja	Dienst ICT	
Maandelijkse Windows Security updates	Maandelijks worden, indien beschikbaar, er door de Dienst ICT security updates op de leverancier PC geïnstalleerd.	Ja	Dienst ICT	

Windows Feature updates	Het Windows besturingssysteem 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	Leverancier	
Apart netwerk segment	Leverancier PC's worden geplaatst in een apart afgeschermd netwerk segment en niet op het netwerk segment van Dienst ICT werkplekken.	Ja	Dienst ICT	
Security baseline	Elke leverancier PC dat wordt aangesloten binnen het Amsterdam UMC domein, zal worden voorzien van de standaard Microsoft beveiliging- instellingen. (Group policy)	Ja	Dienst ICT	
Microsoft Defender installatie beheerd door Amsterdam UMC	Standaard wordt Microsoft defender geïnstalleerd die beheerd wordt door het Amsterdam UMC.	Ja	Leverancier/Dienst ICT	
Uitzonderingsregels antivirus	Vermeld indien van toepassing de antivirus uitzonderingregels.	Ja	Leverancier	

Leveranciers pc checklijst

SCCM	Op elke leverancier PC wordt een SCCM agent geïnstalleerd.	Ja	Dienst ICT	
SCCM rechten	Het SCCM account wordt toegevoegd aan de lokale administrators groep	Ja	Dienst ICT	
Rapid 7	De Rapid7 kwetsbaarheden scanner wordt geïnstalleerd op de leverancier PC. Als er kwetsbaarheden gevonden worden, zal dit aan de afdeling worden doorgegeven.	Ja	Dienst ICT	
Remote toegang	Als er sprake is van remote toegang voor de leverancier, dan moet standaard de remote oplossing van Amsterdam UMC gebruikt worden.	Ja	Dienst ICT	
Plaatsing leverancier PC	De leverancier PC moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met Amsterdam UMC badge met de juiste autorisaties.	Ja	Aanvrager	

De PC configuratie is gehardend en volgt security “best practices van STIG,CIS of de leverancier”. Dit betekent o.a.: - Unieke wachtwoorden. - Alleen noodzakelijk services/protocollen actief. De software geïnstalleerd is altijd up to date	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	Leverancier	
Overige interfaces	Interfaces zoals Wi-Fi, Bluetooth, NFC zijn uitgeschakeld. Als er toch gebruik gemaakt moet worden van deze eerder genoemde interfaces moet dit in overleg met Dienst ICT.	Ja	Leverancier	

Tabel 4 Checklijst Windows 10/11 Professional/Enterprise edities

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

Aanvulling op aansluitvoorwaarden voor leverancier laptops i.c.m. checklijst Windows 10/11 (Professional/Enterprise) LTSC

Maatregel	Beschrijving	Verplicht*	Verantwoordelijk	Gaat de leverancier akkoord met de voorwaarden? (Ja/Nee) Als nee, beschrijf waarom niet. En voorgestelde alternatieven.
Plaatsing laptop	De leverancier laptop moet in een beveiligde ruimte geplaatst worden. Deze ruimte kan alleen geopend worden met Amsterdam UMC badge met de juiste autorisaties.	Ja	Aanvrager	
Fysiek slot op de laptop	Bij de aanschaf van een leverancier laptop moet ook een 'laptop kabel slot' aangeschaft worden. Bij plaatsing van de laptop dient het slot ook direct in gebruik genomen te worden.	Ja	Aanvrager	
Wireless internet laptop	Bij voorkeur wordt de leverancier laptop met een UTP kabel aangesloten. Als dit aantoonbaar niet mogelijk is, wordt de leverancier laptop draadloos verbonden aan een beveiligde WIFI verbinding.	Ja	Leverancier	
USB ethernet aansluiting	Er mag geen gebruik gemaakt worden van USB ethernet aansluitingen.	Ja	Leverancier	
Data back-up op laptop	Data back-up op een leveranciers laptop	Ja	Aanvrager	

	wordt niet gefaciliteerd.			
--	------------------------------	--	--	--

Tabel 5 Additionele aansluitvoorwaarden t.b.v. laptops i.c.m. Windows 10/11 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 over 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, die dit oppakt met de leverancier.
3. De werkplek wordt beheerd door de afdeling en de leverancier (Volgens 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. De verantwoordelijkheid 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, volgens de geldende aansluitvoorwaarden en afspraken die van tevoren overeengekomen zijn.
6. De Dienst ICT verleent alleen ondersteuning op Rapid 7 software, netwerk connectie en de antivirus applicatie.
7. De Dienst ICT is niet verantwoordelijk voor data verlies op de leverancier PC 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 geldende en de levensduur van de leverancier 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 volgens de aansluitvoorwaarden toont aan hoe de update procedure dan verloopt.
10. Als de werkplek intern verhuist is er een meldplicht vanuit de afdeling dit wordt ook verwerkt in de CMDB (Configuration Management Database).
11. Als er sprake is van een securityincident of datalek op de leverancier PC dan heeft de afdeling een meldplicht naar de Dienst ICT (Voorbeelden: ongeautoriseerd toegang, data verlies etc.). Een uitgebreide uitleg is te vinden in [dit](#) document.
12. Als er afgeweken wordt van de initiële overeenkomst (checklijst) tijdens de levensduur van de leverancier PC, moet dit gemeld worden bij de ICT-Servicedesk.
13. Als er sprake is van (patiënten) data verlies dan is er een meldplicht bij de Functionaris Gegevensbescherming van Amsterdam UMC. Zie [K2](#).

14. Is er een (vermoeden van) securityincident dan is er een meldplicht bij het CERT van Amsterdam UMC.
15. 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.
16. De leverancier PC wordt altijd voorzien van een inventarisatie sticker, deze wordt gebruikt voor de registratie in de CMDB (Configuration Management Database).
17. De Windows updates op de leverancier PC worden standaard uitgevoerd op zondagavond. In overleg kan er afgeweken worden van deze dag en tijdstip.
18. Leverancier PC's mogen alleen aangesloten worden in opdracht van de Dienst ICT.

Over leverancier PC's die niet voldoen aan de overeengekomen voorwaarden of die een securityrisico vormen voor Amsterdam UMC, kan besloten worden om deze (tijdelijk) van het netwerk af te sluiten.

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 boven op deze standaard voorwaarden en zijn van toepassing op leverancier PC's met een Windows computer operatie systeem.
Aanvrager	Met aanvrager wordt bedoeld de contactpersoon van de interne Amsterdam UMC afdeling.
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.
Antivirus	De leverancier PC wordt geleverd met antivirus software. Als dit niet mogelijk is, dan wordt standaard Microsoft defender geactiveerd door de Dienst ICT.
Apart netwerk segment	De leverancier PC wordt in een apart netwerk segment geplaatst, gescheiden van de reguliere Dienst ICT beheerde werkplekken.
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.
OS support	De geleverde leverancier PC moet ondersteund worden door Microsoft, en voorzien van een OS die bedoeld is voor computers.
Rapid 7	Deze tool controleert periodiek of de leverancier PC kwetsbaarheden bevat. Denk aan achterlopen van Windows updates.
SCCM	SCCM of Microsoft endpoint Configuration manager agent wordt geïnstalleerd om de machine te voorzien van updates en tools (Windows defender, Rapid 7)
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. (De link is intern alleen te benaderen, deze kan opgevraagd worden).
Security updates	Maandelijkse veiligheidsupdates die door Microsoft worden uitgebracht moeten binnen 2 weken geïnstalleerd zijn op de leverancier PC.
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.

Meest gestelde vragen

V: Hoe kan ik zien welke versie van Windows ik heb?

A:

1. Druk op de Windows-toets op je toetsenbord of klik op de Startknop linksonder op je scherm om het Startmenu te openen.
2. Typ "Over" en selecteer "Over je PC" uit de zoekresultaten. Je kunt ook op de Windows-toets + I drukken om de Instellingen-app te openen, selecteer vervolgens "Systeem" en klik op "Over" in de linkerzijbalk.
3. In het gedeelte "Over" onder "Windows-specificaties" zie je informatie over je Windows-editie en versie. Het versienummer wordt doorgaans weergegeven als iets als "Versie 21H2" of "Versie 10.0 (Build 19042)".
4. Of volg de instructies hier: [Find information about your device - Microsoft Support](#)

V: Wat betekent toepassingsbeheer?

A: Toepassingsbeheer, vaak aangeduid als whitelisting of blacklisting, is een beveiligingsfunctie in Windows waarmee beheerders kunnen bepalen welke toepassingen mogen worden uitgevoerd op een systeem. Meer informatie vind je hier: [Application Control for Windows - Windows Security | Microsoft Learn](#)

V: Wat bedoel je met een beveiligingsbasislijn (security baseline)?

A: Een beveiligingsbasislijn (security baseline) voor Windows is een set vooraf gedefinieerde beveiligingsconfiguraties die door Microsoft worden aanbevolen om een veilig startpunt te creëren voor computersystemen die Windows-besturingssystemen draaien. Deze basislijnen zijn ontworpen om veelvoorkomende beveiligingsdreigingen en kwetsbaarheden te verminderen door specifieke beveiligingsinstellingen en configuraties af te dwingen. De beveiligingsbasislijn omvat doorgaans aanbevelingen voor instellingen met betrekking tot verschillende aspecten van het besturingssysteem, zoals:

- Gebruikers accountbeheer (UAC)
- Instellingen voor Windows Defender Antivirus
- Configuratie van Windows Firewall
- Accountbeleid (wachtwoordbeleid, beleid voor accountvergrendeling, enz.)
- App Locker- of Windows Defender Application Control-instellingen
- Instellingen voor Windows Update
- Netwerkbeveiligingsinstellingen (zoals SMB- en RDP-instellingen)
- Auditbeleid
- Encryptie-instellingen (zoals Bit Locker)

Microsoft brengt periodiek beveiligingsbasislijnen uit voor verschillende versies van Windows, rekening houdend met opkomende bedreigingen, beveiligingspraktijken en feedback van de beveiligingsgemeenschap. Organisaties kunnen deze basislijnen gebruiken als referentie om hun Windows-systemen veilig te configureren, wat zorgt voor consistentie en naleving van beveiligingsnormen binnen hun omgeving. Dit is verplicht wanneer een leveranciers PC is verbonden met het netwerk van Amsterdam UMC.

V: Wat doet Rapid7?

A: Rapid7 biedt oplossingen voor kwetsbaarheidsbeheer die organisaties helpen bij het identificeren, prioriteren en verhelpen van IT beveiligingskwetsbaarheden in hun IT-infrastructuur. Dit omvat kwetsbaarheidsscans die netwerken, systemen en applicaties scannen om potentiële zwakke punten bloot te leggen.

V: Verstoort Rapid7 de prestaties van een PC?

A: De meerderheid van de 'PC's bij Amsterdam UMC maakt gebruik van de Rapid7-agent. De ervaring van het Amsterdam UMC is dat deze impact minimaal is.

V: De leveranciers PC wordt geleverd met een antivirusoplossing die wordt beheerd door de leverancier.

A: Bij het installeren van de PC op het domein van Amsterdam UMC zal IT-services de Amsterdam UMC Defender-client op de machine installeren en eventuele andere antivirusoplossingen uitschakelen of verwijderen.

V: De leveranciers PC functioneert optimaal alleen met antivirusuitzonderingen.

A: Na de aanschaf van de apparatuur door Amsterdam UMC. Geef je Amsterdam UMC-contactpersoon deze uitzonderingen door.

V: Mag ik ondertekende drivers gebruiken in jullie organisatie?

A: Nee, alle drivers moeten ondertekend (WHQL) zijn door Microsoft. Meer informatie vind je hier: [Signing a Driver for Public Release - Windows drivers | Microsoft Learn](#)

V: Wat is Windows LTSC?

A: Windows LTSC (Long term servicing channel) is een Windows variant die ingezet wordt voor cruciale werkplekken in een organisatie, elke paar jaar komt Microsoft met een nieuwe editie. De versie van Windows heeft ook langere support dan de reguliere versie van Microsoft. Extra informatie:

- [Windows Enterprise LTSC overview | Microsoft Learn](#)
- [Windows 10 - release information | Microsoft Learn](#)

Bijlage voor extra notities

Gebruik de onderstaande tabel om extra informatie kwijt te kunnen

Referentie naar maatregel	Extra commentaar

Ondertekening akkoord door leverancier

Ondertekening akkoord PC leverancier	
Naam leverancier en contactpersoon van de leverancier	
Handtekening	
Datum van ondertekening	

Ondertekening akkoord door afdeling *

Ondertekening akkoord interne afdeling	
Naam contact persoon afdeling	
Handtekening	
Datum van ondertekening	

*De redenen waarom er gevraagd wordt voor ondertekening door een Amsterdam UMC afdeling zijn;

1. De afdeling is op de hoogte welke beheer- en supportafspraken er zijn overeengekomen tussen de verschillende betrokken partijen (Dienst ICT, afnemende afdeling en leverancier).

Het document hoeft niet fysiek ondertekend te worden. Er kan ook via de mail een akkoord afgegeven worden door een bevoegde medewerker.