Checklist new supplier PC

Control document for connecting new supplier workstations

Amsterdam UMC Dienst ICT

Author: ICT Service (Workplace Services Department)

From:	Dienst ICT (Internal IT department of Amsterdam UMC)
To:	Externe Suppliers en afdelingen binnen Amsterdam UMC
Cc.:	
Version:	1.4
Date:	04-03-2024

Table of contents

Introduction

Definition of Supplier PC/Laptop: A computer provided by an external supplier, equipped with applications or peripherals to perform (research) tasks. These PCs or laptops are managed by the external party within the frameworks agreed upon by the purchasing department and the internal IT department of Amsterdam UMC (Dienst ICT).

A supplier-provided PC or laptop can be used when deploying a PC supplied by the ICT Service is not feasible, due to support and certification requirements imposed by the external supplier on the supplier's PC configuration. An example of this is when the supplied PC is included as a component in the medical CE certificate.

A supplier PC or laptop is a Windows PC configuration that forms part of an integrated system, intended for use within Amsterdam UMC. This setup requires a connection to the data network and/or Active Directory. An integrated system consists of an application along with its associated workstation(s) fulfilling roles such as acquisition or data processing stations, typically supplied by an external vendor.

To inform departments and vendors about security policies when connecting supplier PCs or laptops, this document includes a checklist outlining the supplier's compliance requirements. Due to significant differences between Windows 10 (only LTSC)/11 IoT variants (desktop/laptop) and Windows Professional/Enterprise variants (desktop/laptop), the document provides two separate checklists, each detailing specific security requirements. Frequently asked questions regarding this document are listed at the end of this document.

Support for Supplier PCs by the "Dienst ICT": Support for supplier PCs is limited. The products supported by the ICT Service are listed in Table 1: Support for Supplier PCs.

Supported products	Description of the support service	Department that provides support for the product
Microsoft Defender from Amsterdam UMC	If the installation of the Amsterdam UMC-managed Defender impacts the functional operation of the supplier's PC, the ICT Service (Dienst ICT) must be contacted. The local installed Defender must have network access to process Defender updates.	Dienst-ICT
Connection to internal network shares	Support configuring network shares.	Dienst-ICT
Rapid 7 vulnerability scanner	If the installation of the vulnerability scanner impacts the functional operation of the supplier PC, the "Dienst ICT" must be contacted.	Dienst-ICT

CMDB registration	The following items are recorded in the CMDB: • PC hardware • Software • PC owner • Software supplier name	Dienst-ICT
Software updates	Assistance with connecting the supplier's PC to the internet for retrieving software updates (e.g., with Microsoft).	Dienst-ICT

Table 1 Support on supplier pc's

Checklist for connecting Windows 10/Windows 11 IoT Enterprise LTSC.

The main contractor (at the ICT Service) of the demand ensures that the checklist below for Windows IoT is completed together with stakeholders: the PC supplier and the relevant department. Make sure to fill in the correct checklist. **For more information, go to chapter:** Frequent asked question

Measure	Description	Mandatory	Responsibility	Does the supplier agree to the terms? (Yes/No) If no, describe why not and propose alternatives.
Comply with connection requirements	Every supplier PC must comply with the current connection requirements established by the ICT Service. The supplier PC meets the requirements from the connection conditions (Internal Link). The document	Yes	Supplier	

	can be provided upon request.			
Feature application control	Application control is a component of Windows IoT. This component must be enabled by default, so that only approved applications can be used.	Yes	Supplier	
Windows defender application control (WDAC)	Only applications and drivers that have been pre-approved by Amsterdam UMC are used.	Yes	Supplier	
Security baseline (GPO)	The Microsoft security baseline is active, including the local firewall, which is configured with the least privileges.	Yes	Supplier	
Filtering or blocking of USB devices	Permission from Amsterdam UMC is required for the use of USB devices on the supplier PC.	Yes	Supplier	
Unified write filter (UWF = kiosk mode)	The supplier PC is in read-only mode by default. Changes to the system are not saved when the machine restarts.	Yes	Supplier	
Network connection	The system is equipped with one network interface. bridge functionality and routing between multiple network segments are not allowed.	Yes	Supplier	

Rapid 7 full scan	The supplied vendor PC allows a vulnerability scan to assess the security level and identify vulnerabilities. The scan is performed using an installed agent, and the results are shared with the vendor, who is requested to take action to resolve any detected vulnerabilities. If there are valid reasons why this is not possible, an agentless scan can be performed.	Yes	Supplier	
Rapid 7 scheduled vulnerability scan	Amsterdam UMC is permitted to periodically perform scans on the device to detect vulnerabilities. This scan is non-authenticating (without logging into the system) and has a low-profile (low intensity) approach to vulnerability scanning. The scan has minimal impact on the system's functionality. The results of this scan are shared with the relevant management department and the ICT security team of Amsterdam UMC.	Yes	Supplier	

The PC configuration is hardened and follows security “best practices from STIG, CIS or the supplier.” This includes: - **Unique passwords.** - **Only necessary services/protocols are active.** - **The installed software is always up to date.**	The use of default passwords and accounts is not allowed within Amsterdam UMC. The account and password must be unique to Amsterdam UMC.	Yes	Supplier	
Other interfaces	Interfaces such as Wi-Fi, Bluetooth, NFC are disabled. If it is necessary to use any of these interfaces, it must be done in consultation with “Dienst ICT.”	Yes	Applicant/Supplier	

Table 2 Checklist connection conditions for Windows 10 IoT

If the connection requirements cannot be fully or partially met, the case must be discussed with the ICT Security Architecture department. If the vendor agrees to the specified conditions, the system may be connected to the network without additional security measures.

Supplement to connection conditions for laptops in combination with Windows 10/Windows 11 IoT enterprise LTSC

Measure	Description	Mandatory	Responsibility	Does the supplier agree to the terms? (Yes/No) If no, describe why not and propose alternatives.
Placement of laptop	The laptop must be placed in a secure area. This area can only be accessed with an Amsterdam UMC badge with the correct authorizations.	Yes	Applicant	

Physical lock on laptop	When purchasing a vendor laptop, a "laptop cable lock" must also be acquired. Upon placing the laptop, the lock is used immediately as well.	Yes	Applicant	
Wireless internet laptop (Exception)	By default, the Supplier laptop is connected with a UTP cable. If the Supplier can demonstrate, after consulting with Amsterdam UMC ICT, that this is not possible, a customized solution will be provided.	Yes	Supplier	
USB network dongles	Network USB dongles are not allowed.	Yes	Supplier	
Data on laptop	Data backup on a vendor's laptop is not facilitated.	Yes	Applicant	

Table 3 Additional connection requirements for laptops in conjunction with Windows with Windows 10/11 IoT

Checklist Windows 10/11 editions (Professional/Enterprise) LTSC

The main contractor (at the ICT Service) of the demand ensures that the checklist below for Windows 10/11 (professional/enterprise) is completed together with stakeholders: The PC supplier and the relevant department. Make sure to fill in the correct checklist. **For more information, go to chapter**: Frequent asked questions

Measure	Description	Mandatory*	Responsible	Does the supplier meet the requirements? (Yes/No) If no, please provide an explanation.
Comply with Amsterdam UMC connection requirements	Every supplier PC must comply with the current connection requirements established by the “Dienst ICT.” The supplier PC meets the requirements from the connection conditions (Internal Link). The document referred to by the link is available upon request.	Yes	Supplier	
OS support	The installed operating system must be supported by Microsoft and designed for PCs. The OS must not have an end-of-support or end-of-life status during the period that the vendor PC is in use at Amsterdam UMC. Therefore, the supplied PCs must include extended support. (Windows 10 may only be provided with the LTSC edition.)	Yes	Supplier	

Drivers and bios updates	During the period that a vendor PC is in use at Amsterdam UMC, the BIOS and drivers must not contain any vulnerabilities.	Yes	Supplier	
Software	Software installed by the vendors on a vendor PC must be updated by the vendor. The software should never be more than 1 version behind, and security updates should be applied immediately.	Yes	Supplier	
Active directory	Supplier PCs are placed in a Suppliers Organizational Unit (OU) within an Amsterdam UMC domain.	Yes	Dienst ICT	
Monthly Windows Security updates	Monthly, security updates are installed on the Supplier PC by the Dienst ICT.	Yes	Dienst ICT	
Windows Feature updates	The Windows operating system for workstations (OS) must be periodically updated by the Supplier to ensure that the installed OS remains within Microsoft's support (Feature updates/Windows as a service process).	Yes	Supplier	

Separate network segment	Supplier PCs are placed in a separate isolated network segment and not on the same network segment of the Dienst ICT managed workstations.	Yes	Dienst ICT	
Security baseline	Every Supplier PC connected within the Amsterdam UMC domain will be equipped with standard Microsoft security settings (Group Policy).	Yes	Dienst ICT	
Microsoft Defender installation managed by Amsterdam UMC	By default, Microsoft Defender is installed and managed by Amsterdam UMC.	Yes	Supplier & Dienst ICT	
Exception rules antivirus software	Specify the antivirus exclusion rules, if applicable.	Yes	Supplier	
SCCM	On every supplier PC, an SCCM agent is installed.	Yes	Dienst ICT	

SCCM rights	SCCM account is added to local administrators' group.	Yes	Dienst ICT	
Rapid 7	The Rapid7 vulnerability scanner will be installed on the vendor PC. If vulnerabilities are found, this will be reported to the internal department.	Yes	Dienst ICT	
Remote access	If remote access for the vendor is required, the standard remote solution of Amsterdam UMC must be used.	Yes	Dienst ICT	
Location supplier pc	The supplier PC must be placed in a secure room. This room can only be accessed with an Amsterdam UMC badge with the appropriate authorizations.	Yes	Applicant	
The PC configuration is hardened and follows security "best practices of STIG, CIS or the supplier." This includes: - **Unique passwords.** - **Only necessary services/protocols are active.** **The installed software is always up to date.**	The use of default passwords and accounts is not allowed within Amsterdam UMC. The account and password must be unique to Amsterdam UMC.	Yes	Supplier	

Other interfaces	Interfaces such as Wi-Fi, Bluetooth, NFC are disabled. If it is necessary to use any of these interfaces, it must be done in consultation with “Dienst ICT.”	Yes	Supplier	

Table 4 Checklist connection conditions for Windows 10/11 Professional/Enterprise editions

* The main contractor discusses the vendor PC with the requester and the vendor during the creation of the procurement dossier. Deviations from the checklist will be indicated to the “Dienst ICT.” The “Dienst ICT” will discuss the deviations and possibilities internally to ensure that the vendor PC is purchased and connected in a safe and functional manner.

Supplement connection conditions for laptops in combination with Supplier PC Windows 10/11(Professional/Enterprise) LTSC

Measure	Description	Mandatory	Responsibility	Does the supplier agree to the terms? (Yes/No) If no, describe why not and propose alternatives.
Placement of laptop	The laptop must be placed in a secure area. This area can only be accessed with an Amsterdam UMC badge with the correct authorizations.	Yes	Applicant	
Physical lock on laptop	When purchasing a vendor laptop, a "laptop cable lock" must also be acquired. Upon placing the laptop, the lock is used immediately as well.	Yes	Applicant	
Wireless internet laptop	By default, the supplier laptop is connected with a UTP cable. If the Supplier can demonstrate, after consulting with “Dienst ICT,” that this is not possible, a customized solution will be explored.	Yes	Applicant	
USB network dongles	Network USB dongles are not allowed.	Yes	Applicant	

Data on laptop	Data backup on a vendor's laptop is not facilitated.	Yes	Applicant	

Table 5 Additional connection requirements for laptops in combination with Windows 10/11 Professional/Enterprise

Agreements, Roles, and Responsibilities

Since various parties (department, “Dienst ICT,” and supplier) are involved in connecting and supporting a new supplier PC, we want to highlight the following agreements, roles, and responsibilities regarding a Supplier PC:

1. All measures mentioned in this document apply to the entire lifespan of the workstation (as long as it is used and/or connected).
2. By installing the Rapid7 "Vulnerabilities" scanner, vulnerabilities on a Supplier PC become visible. These vulnerabilities are monitored by the CERT Team of the ICT Service and reported to the responsible party within Amsterdam UMC.
3. The workstation is managed by the department and the Supplier (according to the agreements made between these two parties regarding the hardware and software on the workstation). The involved prime contractor within the ICT Service will assess the documentation of the agreements during the procurement process.
4. The contractor ship within the ICT Service is divided into two roles (prime contractor and subcontractor):

- Prime contractor: The prime contractor is a team within application services, and the Supplier PC is part of a composite system where an application is always used.
- Subcontractor: The subcontractor is workstation services, and the Supplier PC is a workstation used in a composite system in the role of an acquisition or data processing station. Workstation services will connect the Supplier PC when it meets the checklist described in this document.

5. The “Dienst ICT” acts as a party that connects the Supplier PC according to the applicable connection conditions and agreements that have been agreed upon in advance.
6. The “Dienst ICT” provides support only for Rapid7 software, network connection, and the antivirus application.
7. The “Dienst ICT” is not responsible for data loss on the Supplier PC or for retrieving this data.
8. The Supplier is responsible for upgrading and maintaining a supported operating system (OS). This includes feature updates of, for example, Windows 10/11 (Windows as a service), which are current at the time of delivery and during the lifespan of the Supplier PC.
9. If the supplier does not allow security updates by the “Dienst ICT,” then the Supplier is responsible for updating the workstation according to the connection conditions and demonstrates how the update procedure occurs.

10. If the supplier pc is internally relocated, there is an obligation from the internal department to report this to the “Dienst ICT,” so it can be processed in the CMDB (Configuration Management Database).
11. If there is a security incident or data breach on the supplier PC, then the internal department has an obligation to report it to the “Dienst ICT” (Examples: unauthorized

access, data loss, etc.). Detailed explanations can be found in this document (internal only).

12. If there is a deviation from the initial agreement (checklist) during the lifespan of the Supplier PC, this must be reported to the ICT Service Desk.
13. If there is (suspected) data loss (including patient data), there is an obligation to report to the Data Protection Officer of Amsterdam UMC. See K2.
14. If there is a (suspected) security incident, there is an obligation to report to the CERT of Amsterdam UMC.
15. The supplier PCs are internally monitored by the Rapid7 vulnerability scanner. Findings from this scanner are sent to the department, and it is the responsibility of the department (and supplier) to act.
16. The supplier PC is always provided with an inventory sticker, which is used for registration in the CMDB (Configuration Management Database).
17. Windows updates on the supplier PC are typically performed on Sunday evenings. However, exceptions can be made to this day and time through consultation.
18. Supplier PCs may only be connected upon the instruction of the ICT Service.

Regarding supplier PCs that do not meet the agreed-upon conditions or pose a security risk to Amsterdam UMC, it may be decided to (temporarily) disconnect the supplier pc from the network.

Explanatory glossary

Word and/or concept	Explanation
Applicant	An internal department of Amsterdam UMC.
Connection requirements	Within the Amsterdam UMC network, standard connection conditions are established. Key points in this checklist are extra security measures in addition to these standards and apply to supplier PCs provided with a Windows operating system.
Active Directory connection	De supplier PC is connected to the Amsterdam. UMC domain. It is placed in a separate Organizational Unit, named 'supplier PC.' A distinction is made by division and application.
OS support	The supplier PC provided must be supported by Microsoft and feature an OS intended for computers.
Security updates	Monthly security updates released by Microsoft, must be installed within 2 weeks after release on the supplier pc.
Feature updates	Microsoft must continuously support the installed operating system; this may mean the supplier has to provide the machine with 'Builds.' This allows the PC to receive permanent security updates.
Separate network segment	The supplier PC is placed in a separate network segment, separate from regular workstations managed by "Dienst ICT."
Antivirus	The PC is always provided with a cloud managed Microsoft Defender with standard configuration settings.
Anti-virus exceptions	Sometimes it is necessary to exclude files and folders from scans. The supplier should indicate this in advance.
Security baseline	This is a set of standard security measures defined by Microsoft, which are activated through group policies during the placement of the workstation in the Amsterdam UMC domain. There is a different version for each build. You can find the settings here. (This is an internal link; on request it can be provided)
SCCM	SCCM or Microsoft endpoint configuration manager agent is installed to provide the PC with updates and tools (Microsoft Defender, Rapid 7)
Rapid 7	This vulnerability scanner solution conducts periodic scans to check the Supplier PC for vulnerabilities. For example, checking Windows updates.

Frequent asked questions

Q: How can I see which version of Windows I have?
A:

1. Press the Windows key on your keyboard or click the Start button at the bottom left of your screen to open the Start menu.
2. Type "About" and select "About your PC" from the search results. You can also press the Windows key + I to open the Settings app, then select "System" and click on "About" in the left sidebar.
3. In the "About" section under "Windows specifications," you will see information about your Windows edition and version. The version number is typically displayed as something like "Version 21H2" or "Version 10.0 (Build 19042)".

Q: What does application control mean?
A: Application control, often referred to as allow-listing, is a security feature in Windows that allows administrators to determine which applications are allowed to run on a system. More information can be found here: Application Control for Windows - Windows Security | Microsoft Learn

Q: What do you mean by security baseline?
A: A security baseline for Windows is a set of predefined security configurations recommended by Microsoft to create a secure starting point for computer systems running Windows operating systems. These baselines are designed to reduce common security threats and vulnerabilities by enforcing specific security settings and configurations. The security baseline typically includes recommendations for settings related to various aspects of the operating system, such as:

- User Account Control (UAC)
- Windows Defender Antivirus settings
- Windows Firewall configuration
- Account policies (password policy, account lockout policy, etc.)
- App Locker or Windows Defender Application Control settings
- Windows Update settings
- Network security settings (such as SMB and RDP settings)
- Audit policy
- Encryption settings (such as BitLocker)

Microsoft periodically releases security baselines for different versions of Windows, taking into account emerging threats, security practices, and feedback from the security community. Organizations can use these baselines as a reference to configure their Windows systems securely, ensuring consistency and compliance with security standards within their environment. This is mandatory when a Supplier PC is connected to the Amsterdam UMC network.

Q: What does Rapid7 do?
A: Rapid7 provides vulnerability management solutions that help organizations identify, prioritize, and remediate security vulnerabilities in their IT infrastructure. This includes vulnerability scans that scan networks, systems, and applications to expose potential weaknesses.

Q: Does Rapid7 impact PC performance?
A: The majority of PCs at Amsterdam UMC use the Rapid7 agent. The experience of Amsterdam UMC is that its impact is minimal.

Q: The Supplier PC comes with an antivirus solution managed by the Supplier.
A: When installing the PC on the Amsterdam UMC domain, IT services will install the Amsterdam UMC Defender client on the machine and disable or remove any other antivirus solutions.

Q: The Supplier PC functions optimally only with antivirus exceptions.
A: After the purchase of the equipment by Amsterdam UMC, provide these exceptions to your Amsterdam UMC contact person.

Q: Can I use signed drivers in your organization?
A: No, all drivers must be signed (WHQL) by Microsoft. More information can be found here: Signing a Driver for Public Release - Windows drivers | Microsoft Learn

Q: What is Windows LTSC?
A: Windows LTSC (Long-Term Servicing Channel) is a Windows variant used for critical workstations within an organization. Microsoft releases a new edition every few years. This version of Windows also has longer support compared to the regular Microsoft version.

Additional information:

- Windows Enterprise LTSC overview | Microsoft Learn
- Windows 10 - release information | Microsoft Learn

Space for additional comments

Please use this table to provide extra information or comments.

Measure reference	Additional comments

Signature for agreement supplier

Sign for approval supplier	
Name supplier / name supplier employee	
Signature	
Date of signature	

Sign for approval internal department*

Sign for approval internal department	
Name employee Amsterdam UMC	
Signature	
Date of signature	

*The reasons why signing by an Amsterdam UMC department is requested are:

1. The department is aware of the management and support agreements that have been agreed upon between the various involved parties (ICT Service, receiving department, and Supplier).

The document does not need to be physically signed. Agreement can also be given via email by an authorized employee.