Bijlage I.

Aansluitvoorwaarden apparatuur op de ICT–infrastructuur

Dit document beschrijft de aansluitvoorwaarden voor alle fysieke- en virtuele apparatuur op de ICT-infrastructuur van Amsterdam UMC. Het beleidskader waarbinnen deze voorwaarden zijn opgesteld, is opgenomen in het document '[Beleid aansluiten apparatuur op de ICT-netwerkinfrastructuur]'.

> Noot: Bij sommige voorwaarden is aangegeven dat in overleg met Dienst ICT van de voorwaarde kan worden afgeweken. Wanneer een leverancier daarvan gebruik wil maken, dient hij dat vóór of tijdens de offertefase kenbaar te maken. Een alternatieve oplossing dient vóór of na de offertefase geaccepteerd te zijn door Dienst ICT.
> Als een leverancier de akkoordverklaring kan overleggen, voldoet deze aan de gestelde voorwaarde. Wanneer een leverancier dit niet tijdig meldt of geen akkoord heeft, voldoet deze niet aan de voorwaarde.

Inhoud

1. Hardware en plaatsing

ASV110 Dienst ICT sluit als enige netwerkapparatuur aan op het ICT-netwerk.

Beschrijving	Onder netwerkapparaten vallen alle apparaten waarvan het primaire doel is om netwerkfunctionaliteit te leveren. Deze apparaten oefenen rechtstreeks invloed uit op het functioneren van het ICT-netwerk. Netwerkapparaten worden uitsluitend door dienst ICT aangeschaft en geïnstalleerd. Alleen op die manier kan de stabiliteit van het ICT-netwerk voldoende worden geborgd. Een niet-uitputtende lijst van voorbeelden: switch, router, firewall, draadloze toegangspunten (Wireless Access Point of WAP), modem, maar ook geïnstalleerde software die als netwerkservice fungeert tussen twee netwerkaansluitingen, bijvoorbeeld Windows ICS (Internet Connection Sharing).
Rationale	De netwerkfunctionaliteit vormt het hart van een stabiele infrastructuur.
Consequenties	Bij behoefte aan netwerkapparatuur neemt de aanvrager contact op met dienst ICT. Ook wanneer een leverancier als onderdeel van een complex (medisch gecertificeerd) ICT-systeem een netwerkvoorziening aanbiedt, is nader overleg met dienst ICT nodig. Mogelijk kan dan toch gebruikgemaakt worden van bestaande voorzieningen. Zo niet, dan kan het systeem alleen met speciale maatregelen worden geïnstalleerd, zoals plaatsing in een aparte zone.

ASV120 Apparatuur wordt uitsluitend met goedgekeurde kabels aangesloten.

Beschrijving	Apparaten die bedraad worden aangesloten, worden bij voorkeur aangesloten met kabels die door Amsterdam UMC zijn geselecteerd en aangeschaft. Wanneer een leverancier eigen kabels meeneemt, is vooraf goedkeuring door dienst ICT nodig.
Rationale	Er zijn in de markt vele typen UTP-, DAC- en fiberkabels beschikbaar die niet allemaal voldoen aan de kwaliteitseisen die Amsterdam UMC daaraan stelt. Kabels van onvoldoende kwaliteit kunnen leiden tot verstoringen op het netwerk.
Consequenties	Gebruik bij voorkeur kabels die door Amsterdam UMC beschikbaar zijn gesteld. Deze zijn via de ICT-Servicedesk te verkrijgen. Wanneer een leverancier een systeem inclusief kabels levert, verifieert dienst ICT de kabels vooraf.

ASV130 Apparatuur aansluitingen worden pas geactiveerd na volledige oplevering van de betreffende aansluiting.

Beschrijving	De aansluiting (UTP-eindaansluiting of Telecom Outlet (TO)) is na formele oplevering inclusief de bijbehorende gegevens in beheer bij ICT. De juiste werking is daarmee gewaarborgd en de correcte ruimtegegevens zijn bekend.
Rationale	Aansluitingen waarvan geen meetrapporten zijn opgeleverd en/of waarvan de bijbehorende ruimtegegevens niet bekend zijn, kunnen niet worden beheerd. Een gebruiker kan in dat geval ook niet worden getraceerd.
Consequenties	Gebruik altijd aansluitingen die formeel aan ICT zijn opgeleverd en correct zijn geadministreerd.

ASV140 In datacenters worden uitsluitend apparaten met dubbele voeding en dubbele netwerkaansluiting geplaatst.

Beschrijving	Apparaten (onder andere servers) in de datacenters worden alleen toegestaan wanneer ze qua netwerk en voeding redundant worden aangesloten.
Rationale	Onderhoud aan netwerk of stroomvoorziening kan zo zonder downtijd en zonder moeizame afstemming van service windows worden uitgevoerd.
Consequenties	Uiterlijk bij plaatsing wordt geverifieerd dat de dubbele voeding en redundante netwerkaansluiting aanwezig zijn, en worden beide in gebruik gesteld. Twee apparaten (onder andere servers) die een enkelvoudige voeding en/of netwerkaansluiting hebben, kunnen nog steeds een hoog-beschikbare oplossing vormen. Deze oplossing kan worden geplaatst wanneer akkoord wordt gegaan met de consequenties. Deze worden meegenomen in de SLA. Uitgangspunt is dat een enkelvoudige voeding en/of netwerkcontroller geen belemmering vormt om onaangekondigd beheer uit te voeren waarbij zowel een enkele stroomvoorziening als één van de netwerkaansluitingen kan worden onderbroken.

ASV150 Het type netwerkaansluiting in het datacenter wordt vooraf afgestemd met dienst ICT.

Beschrijving	Het type netwerkaansluiting in het datacenter dient van tevoren te worden bepaald en afgesproken.
Rationale	In de datacenters van Amsterdam UMC worden afhankelijk van de locatie nog verschillende aansluitingen gebruikt (SFP+ of UTP).
Consequenties	Gebruik altijd aansluitingen die formeel met dienst ICT zijn afgestemd.

ASV160 Apparatuur die in datacenters wordt geplaatst, is 'rack-mounted'.

Beschrijving	Apparatuur die in een Amsterdam UMC-datacenter wordt geplaatst, dient rack-mounted te zijn.
Rationale	De datacenters bevatten kasten van het formaat 19 inch. De diepte van de kasten kan per datacenter verschillen; apparatuur die dieper is dan 90 cm dient daarom te worden afgestemd met dienst ICT.
Consequenties	Plaatsing van apparatuur in een datacenter van Amsterdam UMC dient te allen tijde te worden afgestemd met dienst ICT.

ASV170 Client Access-aansluitingen worden uitsluitend aangeboden op basis van 1Gb Ethernet UTP-koperkabels.

Beschrijving	Er zijn meerdere typen Ethernet-bekabeling mogelijk. Amsterdam UMC is volledig gestandaardiseerd op UTP-bekabeling.
Rationale	Standaardisatie van de gebouwbekabeling.
Consequenties	Gebruik altijd apparatuur die geschikt is voor aansluiting op het campusnetwerk van Amsterdam UMC.

2. Instellingen algemeen (datacenter & endpoints in de accesslaag)

ASV210 Het ICT-netwerk gebruikt het IP-netwerkprotocol conform RFC 793 en RFC 791.

Beschrijving	Over het gehele ICT-netwerk wordt het TCP/IP-netwerkprotocol gehanteerd conform RFC 793 en RFC 791 (en de daaropvolgende updates). Subnetten en unicast-routering worden ondersteund. IPv6 wordt niet ondersteund.
Rationale	Het netwerk is geoptimaliseerd op deze protocollen. Andere protocollen kunnen onderlinge verstoringen veroorzaken.
Consequenties	Het apparaat wordt ingesteld op de genoemde protocollen. Neem contact op met dienst ICT indien afwijkende protocollen noodzakelijk zijn. Wanneer multicast vereist is, kan dit in overleg met dienst ICT worden ingesteld.

ASV220 Elk apparaat wordt vóór aansluiting ingesteld op automatische configuratie met DHCP.

Beschrijving	Alle endpoints worden ingesteld op automatische configuratie met DHCP (Dynamic Host Configuration Protocol) voordat ze worden aangesloten op het netwerk.
Rationale	Het automatisch configureren van de netwerkparameters verkleint de kans op fouten en daarmee het risico op verstoringen op het netwerk. Bovendien vereenvoudigt dit de administratie van dienst ICT.
Consequenties	Het apparaat wordt ingesteld op automatische configuratie. Indien het apparaat daar niet op kan worden ingesteld, configureert dienst ICT (Netwerkbeheer) het apparaat ter voorbereiding op de aansluiting en neemt het op in de administratie.

ASV230 Communicatie op het ICT-netwerk vindt plaats op basis van DNS (Domain Name System).

Beschrijving	Communicatie met apparaten vindt op het ICT-netwerk niet rechtstreeks op IP-adres plaats, maar via de door dienst ICT beheerde DNS-service. Met die service worden de logische namen van apparaten vertaald naar het IP-adres. Bij voorkeur wordt de FQDN (hostnaam plus domeinnaam) gebruikt.

Rationale	Dit verhoogt de flexibiliteit van het netwerk en daarmee de beheerbaarheid. Apparaten kunnen andere IP-adressen toegewezen krijgen, zolang de DNS-naam maar naar het juiste apparaat verwijst. Daarnaast is er een beveiligingsaspect. Malware manipuleert vaak DNS-instellingen om controle te krijgen over de verbindingen die een apparaat met computers op het internet maakt.
Consequenties	Connecties van en naar het apparaat maken gebruik van de DNS-service van dienst ICT. Bij dienst ICT is een lijst van actuele servers verkrijgbaar. Is dit niet mogelijk, dan kan in afstemming met dienst ICT een alternatief worden geïmplementeerd.

ASV240 De netwerkpoort (NIC) op het apparaat wordt ingesteld op “auto negotiation”.

Beschrijving	De netwerkpoort van het aan te sluiten apparaat wordt op de instelling “auto negotiation” gezet. Voor locatie VUmc geldt in 2020 een overgangsregeling. Neem contact op met de ICT-Servicedesk voor nadere informatie.
Rationale	Het ICT-netwerk van Amsterdam UMC is geoptimaliseerd op de instelling “auto negotiation”. Andere instellingen kunnen leiden tot een verminderde beschikbaarheid van het apparaat. Ook het foutzoeken wordt hierdoor gecompliceerder.
Consequenties	Sluit alleen apparaten aan waarvan de netwerkpoort is ingesteld op “auto negotiation”, of op locatie VUmc, de toegewezen instelling. Vereist het apparaat een andere instelling voor goed functioneren, neem dan contact op met dienst ICT voor het vinden van een oplossing.

ASV250 Elk apparaat wordt op het netwerk geïdentificeerd met één hardware-ethernetadres.

Beschrijving	Het ethernetadres fungeert als identificatie van het apparaat op het netwerk. Per aansluiting is slechts één ethernetadres actief. Dit adres wordt na aansluiting niet meer aangepast zonder afstemming met dienst ICT.
Rationale	Het kunnen identificeren en traceren van individuele apparaten is verplicht op grond van wet- en regelgeving. Dienst ICT vervult die taak en houdt daarvoor de administratie bij. Daarnaast helpt een eenduidige identificatie bij het foutzoeken.
Consequenties	Spoofing (aanpassen van het MAC-adres door de gebruiker) is niet toegestaan. Wanneer door bijvoorbeeld onderhoud (vervanging van componenten) het adres verandert, wordt dit in afstemming met dienst ICT uitgevoerd. Daarbij wordt de registratie geactualiseerd. Indien de aard van de apparatuur met zich meebrengt dat het apparaat zich met meer dan één adres kan melden (bijvoorbeeld bij VOIP-telefoons of virtuele servers), wordt hiervan een extra registratie bijgehouden en wordt in samenspraak met dienst ICT bepaald hoe deze systemen op het netwerk worden aangesloten.

ASV260 Apparaten binnen één ruimte worden bij voorkeur in dezelfde zone geconfigureerd.

Beschrijving	Binnen een ruimte worden alle apparaten in dezelfde zone geconfigureerd om verwarring en misverstanden te voorkomen bij het aansluiten op de aansluitpunten. Uitgezonderd hiervan zijn de Amsterdam UMC-datacenters.
Rationale	Er bestaat een risico op aansluiting op een verkeerde zone. Als dat gebeurt, kunnen delen van het apparaat of van de applicaties erop mogelijk niet meer functioneren, en kan ook de informatiebeveiliging niet op het afgesproken niveau worden geborgd.
Consequenties	Indien verschillende zones in één ruimte nodig zijn, kan in overleg met dienst ICT en Huisvesting een oplossing worden gevonden. Een van de mogelijke oplossingen is het markeren van de aansluitpunten en kabels door middel van kleurcodering. Een combinatie van productie- met test- of acceptatiezones is hierbij niet toegestaan.

ASV270 Een netwerk-/IoT-apparaat heeft naast PoE ook een dataverbinding nodig op het netwerk.

Beschrijving	Het apparaat onderhoudt een dataverbinding over het netwerk via de aansluiting; de aansluiting is daarmee niet alleen bedoeld als stroomvoorziening. Dataverkeer omvat gestructureerde data, beelden en stuurstromen voor de aansturing van (delen van) een apparaat.
Rationale	PoE-aansluitingen zijn in principe alleen bedoeld voor IT-/IoT-apparatuur die een ICT-rol vervult in het netwerk en die niet via een standaard 230V-aansluiting kan worden voorzien.

Consequenties	Apparaten die alleen stroomvoorziening nodig hebben, worden op 230V aangesloten. In situaties waarin dat lastig te realiseren is, wordt in overleg met Huisvesting/Facilitair naar een oplossing gezocht.

ASV280 Het gevraagde PoE-vermogen is conform de PoE-standaardisatie.

Beschrijving	PoE-levering is conform de standaarden in IEEE 802.af, IEEE 802.at en IEEE 802.bt type 3 (PoE+). Deels wordt IEEE 802.bt type 4* en Cisco UPOE (PoE++) ondersteund. (*Niet beschikbaar op locatie VUmc.)
Rationale	Dit betreft technische beperkingen van de aansluiting.
Consequenties	Apparaten die niet aan deze standaarden voldoen, worden niet aangesloten. Alleen wanneer het apparaat gebruikmaakt van een PoE-standaard is aansluiting op de PoE-voorziening mogelijk.

ASV290 Per access-verdeler (SER-/FD-kast) wordt niet meer dan het vastgestelde PoE-budget gebruikt.

Beschrijving	Voor elke access-verdeler stelt dienst ICT een maximaal PoE-budget vast. Indien de som van de gebruikte vermogens dit budget dreigt te overschrijden, kunnen geen nieuwe apparaten meer worden aangesloten op die voorziening. Per FD/SER is er ongeveer 1500W aan PoE-vermogen beschikbaar. Hierop is monitoring ingeregeld.
Rationale	Dit waarborgt de veiligheid en de uitbreidbaarheid van de netwerkspecifieke voorzieningen.
Consequenties	Bij projecten en aanvragen voor de aansluiting van een PoE-apparaat wordt eerst nagegaan of het budget op de betreffende aansluitvoorziening beschikbaar is. Zo niet, dan worden er geen nieuwe PoE-apparaten meer aangesloten en wordt in overleg gezocht naar een alternatieve oplossing. Voor de berekening van het totale verbruik wordt uitgegaan van het opgegeven maximale vermogen. Dat wordt ook volledig meegeteld wanneer het betreffende apparaat niet continu dat vermogen gebruikt. Het budget bewaakt de piekbelasting.

3. Aanvullende instellingen draadloos

ASV310 WiFi wordt uitsluitend ingezet voor mobiele systemen.

Beschrijving	Het WiFi-netwerk van Amsterdam UMC is bedoeld voor het aansluiten van mobiele systemen die op meerdere locaties worden gebruikt. Statische systemen worden op het bedrade netwerk aangesloten.
Rationale	Het WiFi-netwerk van Amsterdam UMC is geen vervanging voor een bedrade aansluiting, omdat een bedrade netwerkaansluiting een hogere beschikbaarheid biedt en het WiFi-netwerk een beperktere capaciteit heeft, waardoor beschikbaarheidsrisico's ontstaan. Daarnaast is een draadloze verbinding kwetsbaarder dan een bedrade netwerkaansluiting.
Consequenties	Niet-mobiele systemen worden op het bedrade netwerk aangesloten. Indien nodig worden extra aansluitpunten aangebracht in de ruimte waar de aansluiting nodig is. Mobiele systemen worden aangesloten op het draadloze netwerk dat op de locatie daarvoor beschikbaar is. Daarbij wordt een goedgekeurde vorm van authenticatie toegepast. Bij mobiele systemen met hoge beschikbaarheidseisen kan het beste in overleg met dienst ICT worden nagegaan hoe de beschikbaarheid kan worden geoptimaliseerd.

ASV320 De voorkeur gaat uit naar WiFi-frequentieband A (5 GHz).

Beschrijving	Het WiFi-netwerk van Amsterdam UMC werkt op verschillende frequentiebanden: • BG-band (2,4 GHz) • A-band (5 GHz) De voorkeur gaat uit naar gebruik van de A-band. Bedrijf kritische toepassingen worden bij sterke voorkeur alleen in de A-band ontsloten. Niet-bedrijf kritische apparaten kunnen op de BG-band worden aangesloten (niet-overlappende kanalen 1, 6 en 11).
Rationale	Bedrijf kritische toepassingen worden in de A-band ontsloten, omdat deze frequentieband beter gereguleerd is dan de BG-band en over meer kanalen beschikt. Hierdoor is de betrouwbaarheid van de aangeboden diensten via het WiFi-netwerk groter dan op de BG-band.

Consequenties	Het aan te sluiten apparaat wordt geconfigureerd voor de A-band. Indien het geen bedrijf kritisch apparaat betreft, wordt gebruikgemaakt van de niet-overlappende kanalen 1, 6 en 11.

ASV330 Client devices voor bedrijf kritische toepassingen voldoen aan vastgestelde eisen.

Beschrijving	Systemen die met het draadloze netwerk worden verbonden voor bedrijf kritische toepassingen, dienen aan de volgende eisen te voldoen: • Ze ondersteunen U-NII-1 en de DFS-banden U-NII-2 en U-NII-2 extended, zodat de beschikbare bandbreedte maximaal wordt benut. • Ze maken gebruik van het 802.1x-protocol. • Ze voldoen aan de door de WiFi Alliance gestelde WiFi-certificering (zie https://www.wi-fi.org/certification) met bijbehorend logo:
Rationale	Hiermee kan worden voldaan aan de basisvoorwaarden voor beschikbaarheids- en vertrouwelijkheidseisen.
Consequenties	Indien de leverancier bij levering van een complexe configuratie hiervan moet afwijken, kan in overleg met dienst ICT worden nagegaan op welke wijze (bijvoorbeeld met extra voorzieningen) de oplossing mogelijk alsnog kan worden geïnstalleerd.

ASV340 WiFi-clients worden onderling gescheiden van elkaar aangesloten.

Beschrijving	Clients die verbonden zijn op hetzelfde SSID kunnen elkaar niet rechtstreeks benaderen.
Rationale	Om WiFi-clients te beschermen tegen onderlinge besmettingen en/of ongeoorloofde connectiviteit wordt er geen IP-verkeer tussen draadloze clients toegestaan.
Consequenties	Indien er toepassingen worden gebruikt op een draadloos platform die dergelijk verkeer vereisen, kan in overleg met dienst ICT worden vastgesteld hoe dit wordt ingericht.

ASV350 Dienst ICT heeft het exclusieve eigenaarschap over de WiFi-frequentiebanden in de 2,4 en 5 GHz.

Beschrijving	Om de dienstverlening van een centraal WiFi-netwerk van Amsterdam UMC te kunnen garanderen, is het uitstralen en aanbieden van WiFi-SSID's en het gebruik van alle WiFi-kanalen en -banden uitsluitend voorbehouden aan dienst ICT. Ook niet-WiFi-systemen mogen geen gebruik maken van deze frequenties. Hiervan kan uitsluitend worden afgeweken indien de toepassing WiFi-connectiviteit via de door Amsterdam UMC aangeboden infrastructuur niet ondersteunt. Over de inrichting moet met dienst ICT worden afgestemd en de in ASV355 genoemde punten dienen te zijn opgevolgd.
Rationale	De primaire dienstverlening van het ziekenhuis is deels afhankelijk van het centraal aangeboden WiFi-netwerk. Dit kan alleen onverstoord worden gegarandeerd indien de bijbehorende kanalen en banden ook in eigendom zijn van dienst ICT.
Consequenties	Het gebruik van WiFi-kanalen wordt vastgesteld na overleg met dienst ICT.

ASV355 Bij afwijking van ASV350 (lokaal WiFi) gelden vastgestelde overlegpunten en regels.

Beschrijving	De logische naamgeving van het WiFi-netwerk (SSID) wordt in overleg met dienst ICT bepaald. Indien mogelijk wordt de SSID ook als "hidden" aangeboden. Authenticatie en encryptie vinden plaats op basis van WPA2-PSK of WPA3-SAE. Het gebruik van één 5 GHz- of 6 GHz-channel wordt bepaald in overleg met dienst ICT. Het zendvermogen wordt beperkt tot wat voor de betreffende toepassing minimaal nodig is. Te allen tijde dient de Nederlandse wet- en regelgeving te worden gevolgd.
Rationale	De primaire dienstverlening van het ziekenhuis is deels afhankelijk van het centraal aangeboden WiFi-netwerk. Dit kan alleen onverstoord worden gegarandeerd indien de bijbehorende kanalen en banden ook in eigendom zijn van dienst ICT.
Consequenties	Het gebruik van WiFi-kanalen wordt vastgesteld in overleg met dienst ICT.

ASV360 Authenticatie en autorisatie voldoen aan de vastgestelde eigenschappen.

Beschrijving	IEEE 802.1x WPA2-Enterprise authenticatie en autorisatie is op verschillende manieren mogelijk. De voorkeur gaat uit naar gebruik van: 1a – PEAP-MSCHAPv2 1b – EAP-TLS Alleen als WPA2-Enterprise niet mogelijk is, mag met toestemming gebruikgemaakt worden van WPA2-Personal (PSK). Daarbij moeten alle ASCII-characters inclusief “specials” mogelijk zijn.
Rationale	De autorisatie en authenticatie van een WiFi-client zijn cruciaal voor de beveiliging van het WiFi-netwerk.
Consequenties	Clients die niet aan deze beveiligingseis kunnen voldoen, kunnen niet in het WiFi-netwerk worden opgenomen.

ASV370 Op het WiFi-netwerk wordt encryptie toegepast conform de vastgestelde eigenschappen.

Beschrijving	Op de data die over het WiFi-netwerk van Amsterdam UMC wordt verstuurd, dient encryptie te worden toegepast. Hierbij wordt het IEEE 802.11 AES-CCMP protocol voorgeschreven. WPA en TKIP worden niet toegestaan omdat deze niet het vereiste beveiligingsniveau kunnen garanderen.
Rationale	De encryptie op de data van een WiFi-client is cruciaal voor de beveiliging van het WiFi-netwerk.
Consequenties	Clients die niet aan deze beveiligingseis kunnen voldoen, kunnen niet in het WiFi-netwerk worden opgenomen.

4. Inrichting en gebruik

ASV410 Dienst ICT voert de regie over het beheer van het besturingssysteem op aangesloten apparatuur.

Beschrijving	Dienst ICT voert de regie over het beheer van het besturingssysteem op de aangesloten apparatuur.
Rationale	Besturingssystemen zijn door hun aard gevoeliger voor beveiligingslekken. Om het vereiste hoge beveiligingsniveau te kunnen handhaven, is het van belang dat updates en patches in korte tijd infrastructuur breed worden uitgevoerd.
Consequenties	Dit punt betreft alle aangesloten apparatuur, ongeacht de wijze van financiering. Vóór de installatie maakt dienst ICT werkafspraken met de aanvrager over het beheer van het besturingssysteem. Bij voorkeur verzorgt dienst ICT zelf het beheer (updates, upgrades en patches). Dit kan ook een decentrale beheerder betreffen, dat wil zeggen een beheerder buiten dienst ICT inclusief (SBI-)MT, onder regie van dienst ICT. Indien het praktisch niet mogelijk is dat dienst ICT het beheer verzorgt (bijvoorbeeld bij levering en beheer van complexe systemen inclusief een ICT-component), worden er met dienst ICT beheerafspraken gemaakt die invulling geven aan het doel om snel infrastructuur breed updates, upgrades en patches uit te voeren. Dienst ICT komt daarbij maatregelen overeen om toezicht en controle op het beheer te kunnen uitvoeren.

ASV420 Aangesloten apparaten zijn voorzien van actieve anti-malwaresoftware.

Beschrijving	Elk apparaat is voorzien van centraal beheerde anti-malwaresoftware. Dit betekent dat dienst ICT de software actueel houdt en tijdig voorziet van de laatst bekende malwareprofielen.
Rationale	Apparaten zonder actieve anti-malwaresoftware en recente updates en patches vormen een beveiligingsrisico. Het centraal beheer borgt dat de anti-malwaresoftware effectief en actueel is.
Consequenties	Bij dienst ICT is op te vragen welke anti-malwaresoftware in gebruik is. Updates en upgrades verlopen via de beheer-tooling die Amsterdam UMC daarvoor inzet. Indien het praktisch niet mogelijk is om de standaard anti-malwaresoftware te gebruiken, wordt met dienst ICT overeengekomen welke andere anti-malwaresoftware wordt gebruikt. Daarbij worden ook maatregelen afgesproken waarmee dienst ICT de goede werking kan controleren. Dergelijke afspraken kunnen ook per netwerkzone worden gemaakt.

ASV430 Het beleid voor inrichting en gebruik van computerfaciliteiten is van toepassing op alle aangesloten apparatuur.

Beschrijving	Ook bij speciale apparatuur met bijzondere functies in het ICT-netwerk van Amsterdam UMC zijn alle bestaande regels voor inrichting en gebruik van toepassing.
Rationale	Zodra een apparaat is verbonden met het ICT-netwerk, wordt het als integraal onderdeel daarvan beschouwd.
Consequenties	Van toepassing is met name het volgende: • Het “Reglement omgang met ICT-voorzieningen”. • Wet- en regelgeving rond privacy en security. Dit betreft NEN 7510, AVG en BIV-classificatie. • Leidraad Medische Technologie. • MDR (Medical Device Regulation).

ASV440 Apparatuur wordt gebruikt binnen de bestaande instellingen van hard- en software.

Beschrijving	Apparaten worden geïnstalleerd met instellingen in de firmware, het besturingssysteem en de software die nodig zijn om de gewenste functionaliteit te kunnen uitvoeren. Die instellingen vormen de grenzen van het gebruik van de betreffende apparatuur.
Rationale	De instellingen zijn gericht op het optimaliseren van de beschikbaarheid van het gehele ICT-netwerk, op beveiliging, kostenefficiënt beheer en/of privacy.
Consequenties	Wanneer in het gebruik tegen de grenzen van de mogelijkheden van het aangesloten apparaat wordt aangelopen, is daar vaak een functionele reden voor. In overleg met dienst ICT kan worden nagegaan of een andere wijze van aansluiten van het betreffende apparaat mogelijk is, waarbij zowel aan de aansluitvoorwaarden wordt voldaan als aan de wens tot het ruimere gebruik ervan.

ASV450 Op aangesloten apparaten wordt uitsluitend goedgekeurde software gebruikt.

Beschrijving	De software die wordt geïnstalleerd, dient te voldoen aan tenminste de volgende randvoorwaarden: • De licentie voor de software is geregeld; • Het betreft legale software; • Er is voorzien in regulier onderhoud van de software; • De software doet aan lifecycle management; • Er is een securitypatchproces actief waarin updates op basis van het risico binnen een bepaalde periode worden geïnstalleerd; • Voor mobiele applicaties geldt dat deze minimaal door de Google Play Store en/of de Apple App Store gecertificeerd dienen te zijn.
Rationale	De wet- en regelgeving voor gebruik van software is onverkort van toepassing. Illegale software (bijvoorbeeld key-generators) bevat bovendien vaak malware. De eis voor mobiele applicaties voorkomt tevens het gebruik van verouderde en/of bèta-libraries en SDK’s.
Consequenties	Benodigde software wordt expliciet getoetst op bovenstaande punten alvorens deze te installeren. Vooraf wordt nagegaan of andere wet- of regelgeving van toepassing is, bijvoorbeeld de MDR. Neem bij twijfel contact op met dienst ICT.

ASV460 Aangesloten apparaten versturen uitsluitend mail via de centrale mailservers.

Beschrijving	Vanuit aangesloten apparaten met mailvoorziening kan alleen mail worden verzonden via Microsoft 365 of de centrale mailservers, dus niet rechtstreeks naar het internet.
Rationale	Wanneer apparaten besmet raken met een computervirus, kunnen ze malware verspreiden of spam versturen. Wanneer dit via de centrale mailserver verloopt, worden deze apparaten direct gedetecteerd en opgeschoond.
Consequenties	Bij het instellen van mail worden de door dienst ICT aangegeven mailservers gehanteerd.

ASV470 Aangesloten apparaten bevatten geen Peer-to-Peer-software (P2P).

Beschrijving	Software voor “Peer-to-Peer”-verbindingen is niet toegestaan in het ICT-netwerk van Amsterdam UMC. Voorbeelden hiervan zijn: Kazaa, LimeWire, eMule en BitTorrent.

Rationale	"Peer-to-Peer" betekent rechtstreekse communicatie tussen twee computers zonder tussenkomst van een server. Het vormt als het ware een tunnel tussen het aangesloten apparaat en een computer op het internet. Los van het verhoogde risico dat illegale bestanden worden gedownload, bestaat het risico dat vertrouwelijke documenten zoals patiëntinformatie vanuit het aangesloten apparaat worden gedeeld.
Consequenties	Indien de leverancier van een systeem speciale P2P-software voorschrijft, neem dan contact op met dienst ICT. In overleg wordt naar een oplossing gezocht die recht doet aan de eisen van de leverancier en aan de beveiligingseisen van het ICT-netwerk.

ASV480 Aangesloten apparaten bevatten uitsluitend door dienst ICT goedgekeurde Remote Access-software.

Beschrijving	Uitsluitend het gebruik van door dienst ICT goedgekeurde Remote Access-software is toegestaan in het ICT-netwerk van Amsterdam UMC.
Rationale	Met dergelijke software geven apparaten toegang van buitenaf zonder gebruik te maken van de beveiligingsvoorzieningen die Amsterdam UMC heeft aangebracht voor externe toegang. Het risico is dat derden hiermee ongecontroleerde toegang krijgen tot het ICT-netwerk.
Consequenties	Dienst ICT biedt voorzieningen die remote access mogelijk maken. Indien de leverancier van een systeem eigen Remote Access-software voorschrijft, neem dan contact op met dienst ICT. In overleg wordt een oplossing gekozen die recht doet aan de eisen van de leverancier en aan de beveiligingseisen van het ICT-netwerk.

ASV490 Aangesloten apparaten voeren geen netwerk- of serverscans uit.

Beschrijving	Apparaten die worden aangesloten, mogen geen netwerk- of poortscans uitvoeren. Onder scanning wordt in dit verband verstaan: het sequentieel aflopen van alle netwerkadressen of netwerkpoorten om deze in kaart te brengen of om te zoeken naar kwetsbaarheden.
Rationale	Het risico bestaat dat met name oudere apparaten als gevolg van een dergelijke scan ophouden te functioneren. Daarnaast kunnen zulke scans worden gebruikt om het netwerk in kaart te brengen (recon). Dit vormt een beveiligingsrisico.
Consequenties	Indien een netwerkscan nodig is voor een dienst, kan dienst ICT dit op een veilige manier uitvoeren.

ASV495 Aangesloten apparaten zijn gehardend.

Beschrijving	De standaardconfiguratie van de meeste besturingssystemen is niet ontworpen met beveiliging als primaire focus. In plaats daarvan zijn standaardinstellingen meer gericht op bruikbaarheid, communicatie en functionaliteit. Hardening is het proces van het uitschakelen of verwijderen van overbodige en/of niet-gebruikte functies, services en accounts, waarmee de beveiliging wordt verbeterd.
Rationale	Het risico bestaat dat er kwetsbaarheden aanwezig zijn in functionaliteiten die niet strikt nodig zijn voor een correcte werking van het apparaat. Hierdoor ontstaat het risico dat deze kwetsbaarheden worden misbruikt en/of dat de stabiliteit of werking van het apparaat negatief wordt beïnvloed.
Consequenties	Dienst ICT controleert frequent of apparatuur voorzien is van de laatste updates en of deze voldoende gehardend is. Hierbij wordt de CIS-baseline als referentiekader toegepast. Wanneer er geen CIS-baseline beschikbaar is, dienen de best practices van de fabrikant te worden gevolgd.

5. Governance en beheer

ASV510 Dienst ICT beheert het netwerk inclusief alle draadloze communicatie.

Beschrijving	Dienst ICT beheert alle bedrade en onbedrade aansluitingen, alle beschikbare WiFi-banden, Bluetooth, Zigbee, RFID en enig ander gebruik van (radio)frequenties voor datacommunicatie.
Rationale	Ten behoeve van de continuïtteitseis is het noodzakelijk het beheer eenduidig te beleggen. Dit geldt ook voor alle draadloze communicatie, om goede verbindingen met minimale interferentie te kunnen waarborgen. De taak is op beide locaties door de Raad van Bestuur toegewezen aan dienst ICT.
Consequenties	Dienst ICT voert de regie op de aansluiting op het netwerk en op alle draadloze communicatie. Gebruik van draadloze communicatie geschiedt altijd in overleg met dienst ICT. Daarbij wordt afgestemd welke frequentiebanden worden gebruikt met welk doel, en welke kanalen beschikbaar worden gesteld.

ASV520 Apparaten die zonder restricties op het ICT-netwerk worden aangesloten, zijn in beheer bij Amsterdam UMC.

Beschrijving	Apparaten die volwaardig gebruik willen maken van het ICT-netwerk van Amsterdam UMC, komen in beheer bij Amsterdam UMC. Bij draadloze aansluiting wordt gedoeld op de SSID's die verbonden zijn met het Amsterdam UMC-netwerk.
Rationale	Het vereiste niveau van informatiebeveiliging kan alleen worden geborgd wanneer alle apparaten die volwaardig van het ICT-netwerk gebruik willen maken, in beheer zijn bij Amsterdam UMC.
Consequenties	Bij aansluiting wordt bepaald wie binnen Amsterdam UMC het beheer op zich neemt. Dit kan een afdeling van dienst ICT zijn of een van de decentrale ICT-medewerkers inclusief (SBI-)MT. Los van het beheer van het apparaat staat het beheer en gebruik van de data op het apparaat. Die data zijn intellectueel eigendom van Amsterdam UMC en alle wet- en regelgeving rond privacy en security geldt onverkort ook voor dat apparaat.

ASV525 Aangesloten apparaten worden bij voorkeur door Amsterdam UMC beheerd.

Beschrijving	Vooral bij samengestelde systemen komt het voor dat de leverancier voorstelt om een ICT-component toe te voegen die door de leverancier wordt beheerd. Voorbeelden zijn: speciale pc's (meestal leveranciers-pc's genoemd) of hosting-/housingservers. Amsterdam UMC streeft ernaar om deze waar enigszins mogelijk te vervangen door intern beheerde servers of pc's, om aansluiting op de reguliere beheer- en beveiligingswerkzaamheden te borgen.
Rationale	Extern beheerde ICT-componenten leveren extra beheercoördinatie op voor Amsterdam UMC en leiden tot extra risico's.
Consequenties	Tijdens het aanschafproces gaat dienst ICT met de opdrachtgever en de leverancier na of en in hoeverre een oplossing met intern beheerde componenten conform de standaard voldoet. De projectarchitect ondersteunt deze discussie. Indien dit niet mogelijk is, heeft Amsterdam UMC bij pc's de voorkeur om deze zelf conform specificaties van de leverancier aan te schaffen en technisch te beheren, waarbij de leverancier uitsluitend de toepassingen beheert. Bij servers wordt afgewogen of de extra beheerlast bij eigen aanschaf opweegt tegen de extra beheerlast bij (gedeeltelijk) extern beheer. Speelt de leverancier nog steeds een rol bij het technisch beheer, dan wordt zo veel als mogelijk aangesloten bij de reguliere beheerprocessen; dit wordt met de leverancier vastgelegd. Punten van afstemming zijn onder andere: afhandeling van incidenten en changes, testvoorzieningen in aansluiting op de OTAP-straat van ICT, beschikbaarheid van de leverancier bij belangrijke changes in de ICT-infrastructuur, lifecycle-onderhoud, beveiligingsborging en AVG-processen.

ASV530 Apparaten die niet in beheer bij Amsterdam UMC komen, worden met restricties op het ICT-netwerk aangesloten.

Beschrijving	Soms kunnen systemen na aansluiting op het ICT-netwerk van Amsterdam UMC niet in beheer worden genomen door Amsterdam UMC. Dit geldt bijvoorbeeld als de leverancier zelf volledig beheer moet houden om het systeem volledig functioneel te houden. Aansluiting en gebruik

	vinden plaats volgens het least-privileged-principe. Dit is erop gericht om het ICT-netwerk veilig, betrouwbaar en kostenefficiënt te houden.
Rationale	Bij beheer in eigen hand kan snel worden gehandeld in geval van optredende risico's. Externe partijen hebben hun eigen agenda met beheerprioriteiten, waardoor het lastiger wordt om snel en adequaat te reageren.
Consequenties	De aanvrager benoemt een beheerder, die tevens als contactpersoon voor dienst ICT optreedt. In geval van incidenten kan dan snel worden gecommuniceerd. De beheerder is verantwoordelijk voor het monitoren van het juist functioneren van de hardware. Eventuele vervangingen vinden in afstemming met dienst ICT plaats. De beperkingen liggen op verschillende vlakken: • Contractueel regelen van de wijze van beheer: aanpak, responstijden en selectie van beheertools. • Beperking van toegang tot de rest van het ICT-netwerk. Het apparaat wordt in de juiste zonen aangesloten en de instellingen in de firewall worden op basis van least privilege ingericht; alleen datgene wat noodzakelijk is voor het functioneren wordt toegestaan. Dit geldt zowel voor toegang tot de rest van het netwerk als tot het internet. • Beperking van de toegang tot de data door de beheerder. De data is intellectueel eigendom van Amsterdam UMC en alle wet- en regelgeving is van toepassing. Alleen toegang die noodzakelijk is voor het beheer wordt toegestaan en vastgelegd in een verwerkersovereenkomst. • Logging en monitoring van beheer- en onderhoudswerkzaamheden. Ook dienst ICT heeft toegang nodig tot deze gegevens. • In bijzondere gevallen kan het apparaat worden afgesloten van het netwerk als dit noodzakelijk is in het belang van Amsterdam UMC. De beheerder wordt daarvan direct op de hoogte gesteld. • Zonering – plaatsing in een afgescheiden netwerksegment zodat uitsluitend die apparaten bereikt kunnen worden waarvoor de leverancier is geautoriseerd. • Remote access, indien nodig, via een gestandaardiseerde oplossing (bijvoorbeeld Bomgar Remote Access).

ASV535 Data-uitwisseling en aansluiting op de AD vereisen extra voorzieningen op een leveranciers-pc.

Beschrijving	Uitgangspunt voor aansluiting van een leveranciers-pc is volledige isolatie. Vaak voorkomende aanvullende wensen zijn echter data-uitwisseling met andere systemen (van Amsterdam UMC) en/of aansluiting op de Active Directory. Daarvoor zijn meestal voorzieningen op de leveranciers-pc zelf nodig.
Rationale	Extern beheerde leveranciers-pc's vormen risico's voor de veiligheid en continuïteit van de ICT-infrastructuur, en omgekeerd.
Consequenties	Bij aanvullende wensen installeert de leverancier samen met dienst ICT de daarvoor voorgeschreven voorzieningen. De afdeling Werkplekdiensten geeft aan welke voorzieningen dit betreft. In het HLD wordt hiernaar verwezen. Op het moment van schrijven zijn dit de volgende voorzieningen. Voor data-uitwisseling met andere systemen: • Vulnerability Scanner (agent of agentless) • Antivirussoftware • Managementsoftware voor configuratie, patching, updates en monitoring • Restricted Proxy (bij applicatie-updates van internet) Bij connectiviteit met de AD ook: • Besturingssysteem (Microsoft Windows 10 Pro of hoger) • ConfigMgr Agent (voor het faciliteren van beheer) Bij BIV-classificatie Midden of Hoog zijn meer voorzieningen nodig; neem hiervoor contact op met Dienst ICT.

ASV540 (Externe en decentrale) beheerders van aangesloten apparaten voeren het beheer in afstemming met dienst ICT.

Beschrijving	De externe en decentrale beheerders van aangesloten apparaten stemmen de uitvoering van hun beheerwerk af met dienst ICT. Vorm en inhoud van de afstemming worden vastgelegd. Bij decentrale beheerders gebeurt dit in de vorm van een handboek; bij externe beheerders wordt het principe vastgelegd in het contract, waarna nadere afspraken in gezamenlijke werkdocumenten worden gemaakt.
Rationale	Door de toenemende samenhang in het netwerk is afstemming noodzakelijk.
Consequenties	Dienst ICT geeft aan op welke punten afstemming nodig is. Op het moment van vaststelling van deze aansluitvoorwaarden betreft het: • Over en weer afstemmen van security-acties (signaleren van bedreigingen, doorvoeren van patches). • Toegankelijk maken van netwerklogging van het aangesloten apparaat voor dienst ICT. • Toezicht op de data-uitwisseling mogelijk maken voor dienst ICT. • Afstemming van changes zowel op het aangesloten apparaat als in het netwerk met impact op dat aangesloten apparaat. • Afstemming van tijdstippen voor onderhoud met impact op de beschikbaarheid.

ASV550 Aangesloten apparaten worden frequent gescand met een vulnerabilityscanner.

Beschrijving	Dienst ICT maakt gebruik van een vulnerabilityscanner om computers, netwerken en applicaties te beoordelen op kwetsbaarheden. Dit om de hardeningstatus te beoordelen en zwakke punten van een bepaald systeem te ontdekken. Tevens wordt actief gezocht naar onbekende aangesloten apparatuur.
Rationale	Het risico bestaat dat er kwetsbaarheden aanwezig zijn in apparaten waardoor de stabiliteit en/of werking van het apparaat negatief kan worden beïnvloed, of waardoor een apparaat kwetsbaar is voor misbruik of inbreuk.
Consequenties	Dienst ICT controleert frequent alle aangesloten apparatuur op het netwerk. De controle wordt uitgevoerd op het aanwezig zijn van kwetsbaarheden (zero-days), security-updates en op de vraag of apparatuur voldoende gehardend is. Hierbij wordt de CIS-baseline als referentiekader toegepast. Geconstateerde afwijkingen worden gerapporteerd en dienen te worden opgelost binnen een vooraf vastgesteld tijdsbestek zoals beschreven in het patchbeleid van Amsterdam UMC.