Aansluitvoorwaarden apparatuur op de ICT-infrastructuur

Dit document beschrijft de aansluitvoorwaarden voor alle fysieke- en virtuele apparatuur op de ICT-infrastructuur van Amsterdam UMC. Indien het gaat om een rackhostingdienst, dan wordt de intake via een apart proces door de dienst ICT uitgevoerd, waarbij specifieke aansluitvoorwaarden gelden. Het beleidskader waarbinnen deze voorwaarden opgesteld zijn, is opgenomen in het document 'Beleid aansluiten apparatuur'. Dit document is op Kwaliteitsnet en Kwadraet (of de opvolger hiervan) te vinden.

Hardware en plaatsing

ASV110 Netwerkapparatuur wordt alleen door de Dienst ICT aangesloten

Beschrijving	Onder netwerkapparaten vallen alle apparaten waarvan het primaire doel is om netwerkfunctionaliteit te leveren. Daarmee oefenen ze rechtstreeks invloed uit op het functioneren van het ICT-netwerk. Netwerkapparaten worden alleen aangeschaft en geïnstalleerd door de Dienst ICT. Alleen op die manier kan de stabiliteit van het ICT-netwerk voldoende geborgd worden. 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 contact opnemen met de Dienst ICT. Ook wanneer een leverancier als onderdeel van een complex (medisch gecertificeerd) ICT-systeem een netwerkvoorziening bevat, is nader overleg met de Dienst ICT nodig. Wellicht kan toch gebruikgemaakt worden van bestaande voorzieningen. Zo niet, dan kan er alleen met speciale maatregelen, zoals bv. plaatsing in een aparte zone, geïnstalleerd worden.

ASV120 Aansluiten van apparatuur vindt uitsluitend plaats met goedgekeurde kabels

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

ASV130 Activeren van apparatuuraansluitingen vindt plaats 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 waar geen meetrapporten van zijn opgeleverd en/of de bijbehorende ruimtegegevens niet bekend zijn kunnen niet worden beheerd. Een gebruiker kan dan ook niet worden getraceerd.
Consequenties	Gebruik altijd aansluitingen die formeel aan ICT zijn opgeleverd en correct zijn geadministreerd.

ASV140 In datacenters worden alleen apparaten met dubbele voeding en dubbele netwerkaansluiting geplaatst

Beschrijving	Apparaten (servers) in de datacenters worden alleen geplaatst wanneer ze dubbele voeding en een dubbele netwerkcontroller hebben.
Rationale	Het onderhoud aan netwerk of stroomvoorziening kan zonder downtijd en zonder moeizame afstemming van servicewindows uitgevoerd worden.
Consequenties	Uiterlijk bij plaatsing wordt geverifieerd dat de dubbele voeding en redundante netwerkcontroller aanwezig is, en worden beide in gebruik gesteld.

	Bij rackhosting kunnen twee servers die een EV-voeding en/of -netwerkaansluiting hebben, nog steeds een hoog beschikbare oplossing vormen. Deze oplossing kan worden geplaatst wanneer akkoord gegaan wordt met de consequenties. Deze worden meegenomen in de SLA. Uitgangspunt is dat een EV-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.

Instellingen

ASV210 De netwerkpoort ("NIC") op het apparaat wordt ingesteld op "auto negotiation"

Beschrijving	De netwerkpoort van het aan te sluiten apparaat wordt op de keuze "auto negotiation" gezet. Voor de 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 stand "auto negotiation". Andere instellingen kunnen leiden tot een verslechterde beschikbaarheid van het apparaat. Ook foutzoeken wordt hiermee gecompliceerder.
Consequenties	Sluit alleen apparaten aan waarvan de netwerkpoort is ingesteld op "auto negotiation", of, op de locatie VUmc, de toegewezen instelling. Vereist het apparaat een andere instelling voor goed functioneren, neem dan contact op met de Dienst ICT voor het vinden van een oplossing.

ASV220 Apparaten worden op het netwerk geïdentificeerd met één hardware-ethernetadres

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

ASV230 Het ICT-netwerk gebruikt het IP-netwerkprotocol conform rfc793 en rfc791

Beschrijving	Over het hele ICT-netwerk wordt het TCP/IP-netwerkprotocol gehanteerd conform rfc793 en rfc791 (en de daaropvolgende updates). Subnetten en unicast-routering wordt ondersteund. IPv6 wordt niet ondersteund.
Rationale	Het netwerk is geoptimaliseerd op deze protocollen. Protocollen kunnen onderlinge verstoringen geven.
Consequenties	Het apparaat is ingesteld op de genoemde protocollen. Neem contact op met de Dienst ICT indien afwijkende protocollen noodzakelijk zijn. Wanneer multicast vereist is, kan dit in overleg met de Dienst ICT ingesteld worden.

ASV240 Elk endpoint is voor aansluiting ingesteld op automatische configuratie met DHCP

Beschrijving	Alle endpoints zijn 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 de Dienst ICT.
Consequenties	Het apparaat instellen op automatische configuratie. Indien het apparaat daarop niet ingesteld kan worden, zal de Dienst ICT (Netwerkbeheer) het apparaat ter voorbereiding op de aansluiting configureren en opnemen in de administratie.

ASV250 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 de Dienst ICT beheerde DNS-service. Met die service worden de logische namen van apparaten vertaald naar het IP-adres. Bij voorkeur de FQDN (hostnaam plus domeinnaam) gebruiken.
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 security-aspect. 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 de Dienst ICT. Bij de Dienst ICT is een lijst van actuele servers verkrijgbaar. Is dit niet mogelijk, dan kan in afstemming met de Dienst ICT een alternatief geïmplementeerd worden.

ASV260 Apparaten binnen één ruimte zijn bij voorkeur geconfigureerd in dezelfde zone

Beschrijving	Binnen een ruimte worden alle apparaten in dezelfde zone geconfigureerd om verwarring en misverstanden te voorkomen bij het aansluiten op de aansluitpunten.
Rationale	Risico van 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 geborgd worden.
Consequenties	Indien verschillende zones in één ruimte nodig zijn, kan in overleg met de Dienst ICT en Huisvesting een oplossing gevonden worden. Een van de mogelijke oplossingen is het markeren van de aansluitpunten en kabels door bv kleurcodering. Een combinatie van Productie- met Test- of Acceptatiezones is hierbij niet toegestaan.

Aanvullende instellingen draadloos

ASV310 WiFi alleen voor mobiele systemen

Beschrijving	Het WiFi-netwerk is bedoeld voor het aansluiten van mobiele systemen die op meerdere locaties gebruikt worden. Een statisch systeem wordt op het bedrade netwerk aangesloten.
Rationale	Het WiFi-netwerk is geen vervanging voor een bedrade aansluiting omdat een bedrade netwerkaansluiting een hogere beschikbaarheid heeft en het Wifi-netwerk een beperktere capaciteit heeft, waardoor beschikbaarheidsrisico's ontstaan. Daarnaast is een draadloze verbinding kwetsbaarder dan een bedrade.
Consequenties	Niet-mobiele systemen worden op het bedrade netwerk aangesloten. Indien vereist worden extra aansluitpunten aangebracht in de kamer 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 de Dienst ICT nagegaan worden hoe de beschikbaarheid verbeterd kan worden.

ASV320 Voorkeur voor WiFi frequentieband A (5 GHz)

Beschrijving	Het WiFi-netwerk werkt op verschillende frequentiebanden: • BG-band: 2,4 GHz • A-band: 5 GHz De voorkeur gaat uit naar gebruik van de A-band. Bedrijfskritische toepassingen worden bij sterke voorkeur alleen in de A-band ontsloten. Niet-bedrijfskritische apparaten kunnen op de BG-band (niet-overlappende kanalen 1, 6 en 11).
Rationale	Bedrijfskritische 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 dienst(en) via het Wifi netwerk groter dan op de BG-band.
Consequenties	Het aan te sluiten apparaat wordt geconfigureerd voor de A-band. Indien het niet een bedrijfskritisch apparaat betreft, wordt gebruikgemaakt van de niet-overlappende kanalen 1, 6 en 11.

ASV330 Requirements voor client devices van bedrijfskritische toepassingen

Beschrijving	Systemen die met het draadloze netwerk verbonden worden voor bedrijfskritische toepassingen dienen aan de volgende requirements te voldoen: • Ondersteunen U-NII-1 en de DFS-banden U-NII-2 en U-NII-2 extended. Hierdoor wordt de beschikbare bandbreedte maximaal benut. • Gebruik van het 802.1x-protocol • Voldoen aan de door de WiFi-alliance gestelde WiFi-certificering. Dit is hier beschreven: https://www.wi-fi.org/certification en dit is het bijbehorende logo:
Rationale	Het kunnen voldoen aan de basisvoorwaarde voor beschikbaarheids- en vertrouwelijkheidseisen.
Consequenties	Indien de leverancier bij levering van een complexe configuratie hiervan moet afwijken, kan in overleg met de Dienst ICT nagegaan worden op welke wijze (bv met extra voorzieningen) de oplossing alsnog geïnstalleerd kan worden.

ASV340 WiFi-clients worden onderling gescheiden van elkaar aangesloten

Beschrijving	Clients die verbonden zijn op hetzelfde SSID kunnen elkaar niet direct 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 wireless platform die dergelijk verkeer verlangen, kan in overleg met de dienst ICT worden vastgesteld hoe dit zal plaatsvinden..

ASV350 ICT-eigenaarschap op WiFi-frequentiebanden in de 2,4 en 5GHz

Beschrijving	Om de dienstverlening van een centraal AmsterdamUMC-WiFi-netwerk te kunnen garanderen is het uitstralen en aanbieden van WiFi-SSID's en het gebruik van WiFi-kanalen uitsluitend voorbehouden aan de dienst ICT.
Rationale	De primaire dienstverlening van het ziekenhuis is deels afhankelijk van het centraal aangeboden WiFi-netwerk, Dit kan alleen onverstoord worden gegarandeerd, indien de hierbij behorende kanalen ook in eigendom zijn van de dienst ICT.
Consequenties	Het gebruik van WiFi-kanalen wordt vastgesteld in overleg met de dienst ICT.

Inrichting en gebruik

ASV410 De Dienst ICT voert de regie over het beheer van het besturingssysteem

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

ASV420 Aangesloten apparaten zijn voorzien van actieve antimalwaresoftware

Beschrijving	Elk apparaat is voorzien van actieve antimalwaresoftware, dat wil zeggen dat de software actueel gehouden wordt en tijdig voorzien wordt van de laatst bekende malwareprofielen.
Rationale	Apparaten zonder actieve antimalwaresoftware en recente updates en patches vormen een beveiligingsrisico.
Consequenties	De voorkeur gaat uit naar het gebruik van antimalwaresoftware die de Dienst ICT centraal beheert. Bij de Dienst ICT is op te vragen welke antimalwaresoftware in gebruik is. Op het moment van publicatie is dat McAfee en Trend Micro; voor beheerde mobiele devices voorziet MDM in deze functionaliteit. Updates en upgrades lopen via de beheertooling die Amsterdam UMC daarvoor inzet (op het moment van schrijven is dat ePolicy Orchestrator op locatie VUmc). Detecties worden direct doorgegeven aan het CSIRT van Amsterdam UMC. Mocht het praktisch niet mogelijk zijn hiervan gebruik te maken, dan wordt met de Dienst ICT overeengekomen welke andere antimalwaresoftware gebruikt wordt. Daarbij worden ook maatregelen afgesproken waarmee de Dienst ICT de goede werking kan controleren. Zulke afspraken kunnen ook per netwerkzone gemaakt worden.

ASV430 Het beleid voor inrichting en gebruik van computerfaciliteiten is van toepassing

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 verbonden is aan het ICT-netwerk, wordt het als integraal onderdeel daarvan beschouwd.
Consequenties	Van toepassing is met name het volgende: • het “Reglement omgang met ICT” voor beide locaties. Zolang die gedragsregels nog gescheiden zijn, zijn beide van toepassing. Het netwerk is immers al verregaand gekoppeld. Bij eventuele strijdigheden prevaleren de regels van de locatie waar de aansluiting plaatsvindt. • wet- en regelgeving rond privacy en security. Dit betekent NEN7510, AVG en BIV-classificatie. • Convenant Medische Technologie (zie referentie onder aan dit document) • MDR (zie referentie onder aan dit document)

ASV440 Gebruik van apparatuur vindt plaats binnen de bestaande instellingen van hard- en software

Beschrijving	Apparaten worden geïnstalleerd met instellingen in de firmware, het besturingssysteem en de software die nodig is 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 aangelopen wordt, is daar vaak een functionele reden voor. In overleg met de Dienst ICT kan nagegaan worden of een andere wijze van aansluiten van het betreffende apparaat mogelijk is, waarbij zowel voldaan is aan de aansluitvoorwaarden als ook aan de wens tot het ruimere gebruik ervan.

ASV450 Op aangesloten apparaten wordt uitsluitend goedgekeurde software gebruikt

Beschrijving	De software die geïnstalleerd wordt, dient goedgekeurd te zijn. Goedgekeurd houdt in: • de licentie voor die software is geregeld; • het betreft legale software; • er is voorzien in regulier onderhoud van de software; • valt onder lifecyclemanagement; • er is een securitypatchproces actief waarin de updates op basis van het risico binnen een bepaalde periode geïnstalleerd worden.
Rationale	De wet- en regelgeving voor gebruik van software is onverkort van toepassing. Illegale software (bijvoorbeeld “Key-generators”) bevat bovendien vaak malware.
Consequenties	Benodigde software wordt expliciet getoetst op bovenstaande punten alvorens te installeren. Ook wordt vooraf nagegaan of andere wet- of regelgeving van toepassing is, bv MDR. Neem bij twijfel contact op met de Dienst ICT.

ASV470 Aangesloten apparaten versturen uitsluitend mail via de centrale mailservers

Beschrijving	Vanuit aangesloten apparaten met mailvoorziening kan alleen mail verzonden worden via Office365 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 loopt, worden deze apparaten direct gedetecteerd en opgeschoond.
Consequenties	Bij het instellen van mail de door de Dienst ICT aangegeven mailservers hanteren.

ASV480 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 gedownload worden, is er het risico dat vertrouwelijke documenten zoals patiëntinformatie uit het aangesloten apparaat worden gedeeld.
Consequenties	Indien de leverancier van een systeem speciale P2P-software voorschrijft, neem dan contact op met de Dienst ICT. In overleg zal naar een oplossing gezocht worden die recht doet aan de eisen van de leverancier en aan de beveiligingseisen van het ICT-netwerk.

ASV490 Aangesloten apparaten bevatten geen Remote Access-software (die extern te benaderen is)

Beschrijving	Uitsluitend het gebruik van door de Dienst ICT goedgekeurde Remote Access-software is toegestaan in het ICT-netwerk van Amsterdam UMC.
Rationale	Met deze 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	De Dienst ICT biedt voorzieningen die remote access mogelijk maakt. Indien de leverancier van een systeem eigen Remote Access-software voorschrijft, neem dan contact op met de Dienst ICT. In overleg zal een oplossing gekozen worden die recht doet aan de eisen van de leverancier en aan de beveiligingseisen van het ICT-netwerk.

ASV500 Aangesloten apparaten voeren geen netwerk- of serverscans uit

Beschrijving	Apparaten die aangesloten worden, mogen geen netwerk- of poortscans uitvoeren. Onder scanning wordt in dezen verstaan het sequentieel 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 zo'n scan ophouden te functioneren. Daarnaast kunnen zulke scans ook gebruikt worden om het netwerk te leren kennen (recon). Dit is een securityrisico.
Consequenties	Indien er een netwerkscan nodig is voor een dienst, kan de Dienst ICT dit op een veilige manier uitvoeren.

ASV510 Aangesloten apparaten zijn gehardend

Beschrijving	De standaardconfiguratie van de meeste besturingssystemen is niet ontworpen met beveiliging als de 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 apparaten in functionaliteiten die niet strikt benodigd zijn voor een correcte werking van het apparaat. Hierdoor ontstaat een risico dat die misbruikt worden, en/of dat de stabiliteit/werking van het apparaat negatief beïnvloed wordt.
Consequenties	Dienst ICT controleert frequent of apparatuur voorzien is van de laatste updates en of deze voldoende gehardend zijn. Hierbij wordt de CIS-baseline als referentiekader toegepast. Wanneer er geen CIS-baseline beschikbaar is, dienen de best practices van de fabrikant gevolgd te worden. 

Governance en beheer

ASV610 De Dienst ICT beheert het netwerk inclusief draadloze communicatie

Beschrijving	De Dienst ICT beheert alle bedrade en onbedrade aansluitingen, alle beschikbare WiFi-banden, Bluetooth, Zigbee, RFID en enig ander gebruik van (radio)frequenties voor communicatie van data.
Rationale	Ten behoeve van de continuïteitseis 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 in beide locatie door de Raad van Bestuur toegewezen aan de voorlopers van de Dienst ICT.
Consequenties	De Dienst ICT voert de regie op de aansluiting op het netwerk en op alle draadloze communicatie. Gebruik van draadloze communicatie gaat altijd in overleg met de Dienst ICT. Daarbij wordt afgestemd welke frequentiebanden gebruikt worden met welk doel, en welke kanalen beschikbaar gesteld worden.

ASV620 Apparaten die zonder restricties op het ICT-netwerk moeten worden aangesloten, zijn in beheer bij Amsterdam UMC

Beschrijving	Apparaten die een volwaardig gebruik van het ICT-netwerk van Amsterdam UMC willen maken, 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 is bepaald wie binnen Amsterdam UMC het beheer op zich neemt. Dit kan een afdeling van de 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 is in intellectueel eigendom van Amsterdam UMC, en alle wet- en regelgeving rond privacy en security gelden onverkort ook voor dat apparaat.

ASV625 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 beheerd wordt. Voorbeelden: speciale pc's (meestal leveranciers-pc's genoemd) of rackhosting-servers. 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 securitywerkzaamheden 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 de 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. Mocht dit niet mogelijk zijn, dan heeft Amsterdam UMC bij pc's de voorkeur die 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, securityborging en AVG-processen.

ASV630 Apparaten die niet in beheer bij Amsterdam UMC komen, worden met restricties op het ICT-netwerk aangesloten

Beschrijving	Soms kunnen systemen niet in beheer genomen worden bij Amsterdam UMC na aansluiting op het ICT-netwerk van Amsterdam UMC. Dit geldt bijvoorbeeld als de leverancier zelf volledig beheer moet houden om het systeem volledig functioneel te houden. Aansluiting en gebruik vindt 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 gehandeld worden in geval van optredende risico's. Externe partijen hebben hun eigen agenda met beheerprioriteiten, dus zal het lastiger worden om snel en adequaat te reageren.
Consequenties	De aanvrager benoemt een beheerder, die tevens als contactpersoon voor de Dienst ICT optreedt. In geval van incidenten kan dan snel gecommuniceerd worden. De beheerder is verantwoordelijk voor het monitoren van het juist functioneren van de hardware. Eventuele vervangingen vinden in afstemming met de Dienst ICT plaats. De beperkingen liggen op verschillende vlakken: • contractueel regelen van wijze van beheer: aanpak, responstijden, selectie van beheertools. • beperking van toegang tot de rest van het ICT-netwerk. Het apparaat wordt in de juiste zone aangesloten, en de instellingen in de firewall gaan op basis van 'least privilege', dat wil zeggen dat 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 de Dienst ICT heeft toegang nodig tot deze gegevens. • In bijzondere gevallen kan het apparaat afgesloten worden van het netwerk als dit noodzakelijk is in het belang van Amsterdam UMC. De beheerder zal daarvan direct op de hoogte gesteld worden. • Zonering – in een afgescheiden netwerksegment zodat uitsluitend die appraten bereikt kunnen worden waarvoor de leverancier geautoriseerd is • Remote access, indien nodig via gestandaardiseerde oplossing (bv. Bomgar remote access)

ASV635 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 AD. 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 de dienst ICT de daarvoor voorgeschreven voorzieningen. De afdeling Werkplekdiensten geeft aan welke voorzieningen dit betreft. In de 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) • Antivirus (McAfee of getekend contract met abonnement voor andere AV) • Managementsoftware voor configuratie, patching, updates en monitoring • Restricted Proxy (bij applicatie-updates van internet) Bij connectiviteit met AD ook:

	• Operating system software (Microsoft Windows 10 Pro of hoger) • ConfigMgr Agent (voor faciliteren beheer) NB. Bij BIV-classificatie Midden of Hoog zijn meer voorzieningen nodig; zie daarvoor de Matrix Minimale Maatregelen.

ASV640 (Externe en decentrale) beheerders van aangesloten apparaten voeren het beheer in afstemming met de Dienst ICT

Beschrijving	De externe en decentrale beheerders van aangesloten apparaten hebben in de uitvoering van hun beheerwerk afstemming met de Dienst ICT. Vorm en inhoud van de afstemming wordt vastgelegd. Bij decentrale beheerders 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	De Dienst ICT geeft aan op welke punten afstemming nodig is. Op het moment van vaststellen van deze aansluitvoorwaarden betreft het: • Over en weer afstemmen van security-acties (signaleren bedreigingen, doorvoeren patches) • Toegankelijk maken van netwerklogging van het aangesloten apparaat voor de Dienst ICT; • Toezicht op de data-uitwisseling mogelijk maken voor de dienst ICT; • Afstemming van changes zowel op het aangesloten apparaat als ook in het netwerk met impact op dat aangesloten apparaat; • Afstemming van tijdstippen voor onderhoud met impact op beschikbaarheid.

ASV650 Aangesloten apparaten worden frequent met een vulnerabilityscanner gescand

Beschrijving	Dienst ICT zet een vulnerabilityscanner in om computers, netwerken of 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 beïnvloed kan worden of een apparaat kwetsbaar is voor misbruik/inbreuk.
Consequenties	Dienst ICT controleert frequent alle aangesloten apparatuur op het netwerk. Controle wordt uitgevoerd op het aanwezig zijn van kwetsbaarheden (zero-days), security-updates en of apparatuur voldoende gehardend is. Hierbij wordt de CIS-baseline als referentiekader toegepast. Geconstateerde afwijkingen worden gerapporteerd en dienen opgelost te worden binnen een vooraf vastgesteld tijdsbestek zoals beschreven in het patchbeleid van Amsterdam UMC.

Referenties

Titel	Bron
Convenant Medische Technologie	https://www.igj.nl/zorgsectoren/medische-technologie/toezicht-op-veilig-gebruik/convenant
MDR	https://www.rijksoverheid.nl/onderwerpen/medische-hulpmiddelen/nieuwe-wetgeving-medische-hulpmiddelen

Versiebeheer

Datum	Versie	Auteur	Wijzigingen
3-2-2020	0.5	Arie Elsenaar, Ewald Beekman	Eerste uitwerking van een beleidsdocument voor de nieuwe aansluitvoorwaarden van de Dienst ICT
10-3-2020	0.8	Arie Elsenaar	Verwerking alle feedback van reviewers
31-3-2020	0.9	Arie Elsenaar	Verwerking feedback alle beheerteams in afstemming met Arend, Erwin en Ewald
16-4-2020	0.95	Arie Elsenaar	Laatste aanvullingen, opmaak
14-5-2020	0.96	Arie Elsenaar	Aanscherping op basis van MT-feedback
19-5-2020	1.0	Arie Elsenaar	Vastgesteld in het MT van de Dienst ICT
20-10-2020	1.1	Hans vd Heuvel Arend Hollebeek Erwin Wortel Arie Elsenaar	Toegevoegd securitypunten, aansluiting van leveranciers-pc's, zoneringseisen, eisen t.a.v. virtuele servers.