Erasmus MC
Universitair Medisch Centrum Rotterdam

Document	Aansluitvoorwaarden Erasmus MC-netwerk
Versie	11.0
Datum	29 augustus 2024
Opsteller(s)	Pieter van Dorp, Lars Hameeteman, Jasper Klaren, Danjan Mudde
Beheerder(s)	Pieter van Dorp en Danjan Mudde
Opdrachtgever	Bob Maas

Aansluitvoorwaarden Erasmus MC-netwerk

Inhoudsopgave

Revisiedatum: 29-8-2024

Versiebeheer:

Versie datum	Versie	Samenvatting van de aanpassing	Uitgevoerd door
8-4-2021	10.1	802.1x en DNS naamgeving	Danjan Mudde
01-09-2022	10.2	Toevoeging van beschrijving toestaan Multicast binnen netwerk	Danjan Mudde
01-09-2022	10.2	Hoofdstuk nummering aangepast	Danjan Mudde
16-01-2023	10.3	Onder kopje Netwerkaansluiting Power Over Ethernet eis toegevoegd	Danjan Mudde
12-5-2023	10.4	WOL niet meer mogelijk na introductie 802.1x met dynamische VLAN toewijzing	Danjan Mudde
29-8-2024	11.0	Toevoeging TLS protocollen	Danjan Mudde

Document eigenaar: Team netwerkbeheer

1 Algemeen

1.1 Doel

Deze aansluitvoorwaarden beschrijven de spelregels die gelden voor het aansluiten van IT-middelen op de netwerkinfrastructuur van het Erasmus MC (‘Erasmus MC-netwerk’).

Deze spelregels zijn nodig om de prestaties, continuïteit (beschikbaarheid) en veiligheid van deze infrastructuur te garanderen.

1.2 Vaststelling en wijziging

1.2.1 Aansluitvoorwaarden

Deze aansluitvoorwaarden worden vastgesteld door het Management Team (MT) van de Pijler Informatie & Technologie van het Service Bedrijf en bekrachtigd door de Raad van Bestuur. Wijziging of aanpassing van de voorwaarden vindt plaats zodra technische of andere ontwikkelingen dit noodzakelijk maken. In dat geval zal aan het MT van de Pijler Informatie & Technologie van het Service Bedrijf een voorstel hiertoe worden gedaan door de manager van ICT Services.

1.2.2 Uitzonderingen

Over uitzonderingen op de in dit stuk gestelde voorwaarden beslist de leiding van ICT Services na een hiertoe gedaan schriftelijk en gemotiveerd verzoek.

1.3 Publicatie

Deze aansluitvoorwaarden worden gepubliceerd op Intranet, met vermelding van versienummer en datum van vaststelling.

2 Aansluitvoorwaarden netwerkinfrastructuur

2.1 Leeswijzer

In dit hoofdstuk zijn de technische aansluitvoorwaarden uitgewerkt.
De indeling is als volgt:

2.2 algemene aansluitvoorwaarden;

2.3 Te gebruiken protocollen

2.4 aansluitvoorwaarden voor client PC's op het draadgebonden LAN;

2.5 aansluitvoorwaarden voor systemen op draadloze LANs;

2.6 aansluitvoorwaarden voor servers;

2.7 aansluitvoorwaarden voor externe toegang.

Deel 2.2 beschrijft aansluitvoorwaarden die voor **alle systemen en alle domeinen** gelden met als uitzondering 2.2.1 (Netwerk Access Control). Netwerk Access Control geld alleen voor de delen 2.3 en 2.4

Het onderscheid tussen de delen 2.3 / 2.4 en anderzijds deel 2.6 rust op de domeinindeling die is ingesteld ter compartimentering van de netwerk-infrastructuur[1]:

* Delen 2.3 en 2.4 beschrijven de aansluitvoorwaarden voor het **belangrijkste 'gebruikersdomein'** binnen Erasmus MC.
* Deel 2.5 richt zich op de aansluitvoorwaarden voor de **'serverdomeinen'**.

[1] Zie literatuurlijst in de appendix, document 2, "Richtlijn Domeinen en Externe Toegang".

2.2 Algemene aansluitvoorwaarden

Voor **elk systeem** dat gekoppeld wordt aan het Erasmus MC-netwerk (zowel client PC's als servers) gelden de algemene eisen in dit hoofdstuk, in aanvulling op meer gedetailleerde eisen die in volgende hoofdstukken nog worden gesteld.

2.2.1 Het netwerk van het Erasmus MC is onderverdeeld in netwerkzones (geïmplementeerd als zgn. VRF's), waarvan de belangrijkste zijn:

1. intern (default)
2. student
3. externen
4. hotspot
5. patiëntbewaking (draeger)
6. isolatie
7. patient services (patserv)
8. Netsrv (Network services)

Onderstaande eisen gelden voor alle systemen in deze netwerkzones, tenzij anders is aangegeven.

1. **Virus en Malware** bescherming.
    a. Elk systeem moet zijn voorzien van een recent operating system dat actief ondersteund wordt en er dienen maatregelen genomen te worden om er voor te zorgen dat het systeem actief[2] beschermd is tegen virussen en malware. Zowel het operating system als de hierop gebruikte software moeten zijn voorzien van alle actuele (beveiligings)updates.
    b. Deze eis geldt niet voor systemen in de netwerkzones 'hotspot' (4) en 'patiëntbewaking' (5)!
    c.
2. **Software-licenties**.
    a. Toegestaan is alleen installatie en gebruik van software waarvoor een licentieovereenkomst aanwezig is, hetzij bij ICT Services, hetzij op de afdeling zelf.
    b. Deze eis geldt niet voor systemen in de netwerkzone 'hotspot' (4).

[2] onder **'actief beschermen'** wordt verstaan dat de genomen maatregel beschermen tegen kwaadaardig netwerkverkeer en malware
- bij het opstarten van de pc
- bij het lezen of openen van bestanden op interne of externe gegevensbronnen
- bij het downloaden van bestanden van Internet/Intranet of andere externe netwerken waarmee verbinding is opgebouwd (zoals toegestaan binnen deze aansluitvoorwaarden).

3. **TCP/IP**. Alle aangesloten systemen maken uitsluitend gebruik van het IP protocol om toegang te krijgen tot de logische netwerk-infrastructuur.
    a. Om brede connectiviteit te waarborgen beheert ICT Services centrale **DHCP- en DNS servers**. Het gebruik hiervan is verplicht.
    b. Dit betekent:
    - voor DNS wordt uitsluitend gebruik gemaakt van de door het netwerkteam aangewezen centrale servers. Gegevens t.a.v. te gebruiken DNS servers zijn opvraagbaar bij het netwerkteam. DNS servers worden op cliënt systemen automatisch middels het DHCP protocol geconfigureerd;
    - het IP-adres wordt met behulp van '**automatisch opvragen**' verkregen, dat wil zeggen dat het adres dynamisch toegewezen wordt door de centrale DHCP servers.
    c. In afwijking van het bovenstaande kan bij ICT Services een (gemotiveerde) aanvraag worden gedaan voor een **vast IP adres**; een dergelijk vast IP adres kan **alleen** door het netwerkteam van ICT Services worden toegewezen.
    d. Deze eis geldt niet voor systemen in de netwerkzone 'patiëntbewaking' (5).
4. Software dient zó geconfigureerd te worden dat DNS host names worden gebruikt in plaats van IP-adressen.
5. Applicatiesoftware die actief gebruik maakt van IP- en/of Ethernet- **broadcast** is niet toegelaten. Indien bovengenoemde software gebruik maakt van IP- en/of Ethernet-**multicast** is deze alleen toegelaten na overleg met, en goedkeuring van, het netwerkteam van ICT Services.
    a. Wanneer een nieuwe Multicast toepassing is gewenst zal deze nieuwe toepassing voorgelegd moeten worden aan de netwerkarchitecten. Zij bepalen nadat een concept technisch ontwerp is besproken en mogelijk testen zijn uitgevoerd of en op welk wijze de nieuwe multicast toepassing wordt geïmplementeerd;
    b. Wanneer Multicast wordt toegestaan worden multicast adresschema's toegekend door de netwerkarchitecten van het Erasmus MC. Als de apparatuur niet flexibel is om de toegewezen multicast adressen in te voeren wordt multicast niet toegestaan;
6. Het is verboden om software te installeren waarmee andere op het Erasmus MC-netwerk aangesloten gebruikers-PC's kunnen worden benaderd, bestuurd en/of gemanipuleerd. Dit behoudens middelen die door ICT Services worden gebruikt ten behoeve van het beheer van PC's.
7. Elke persoon die in staat wordt gesteld een gekoppeld systeem te gebruiken of bedienen kent en respecteert de vastgestelde **gedragscode** (zie appendix, document 1: "Gedragscode voor het gebruik van computerfaciliteiten van het Erasmus MC").

8. Een op een systeem te configureren DNS hostnaam wordt opgebouwd op basis van een gestandaardiseerde werkwijze. Deze werkwijze is beschreven in het document “Naamgeving systemen Vx.x.docx”. Dit document is opvraagbaar bij het team netwerkbeheer. Het volgen van deze standaard is een eis. Wanneer de naamgeving voor een specifiek systeem nog niet is opgenomen in dit document zal er op basis van bestaande en nieuw aan te brengen variabelen een nieuwe standaard worden gemaakt voor het specifieke device. Deze eis geldt niet voor systemen in de netwerkzone ‘hotspot’ (4).

2.2.2 NAC Netwerk Access Control (802.1x)

Het Erasmus MC maakt voor de toegang tot het netwerk (bedraad en draadloos) gebruik van een Netwerk Access Control systeem (NAC). Dit systeem bepaalt op basis van meerdere kenmerken of toegang tot het netwerk is toegestaan. Om een systeem te verbinden met de netwerk infrastructuur van Erasmus MC, dient men in het ontwerp van een dienst of aanschaf van systemen rekening te houden met 802.1x netwerkauthenticatie. Dit is een eis.

De volgende authenticatiemethoden worden door het Erasmus MC ondersteund waarbij de standaard EAP is:

EAP

Een aan te sluiten systeem ondersteunt netwerkauthenticatie op basis van 802.1x middels EAP. (RFC 3748) Niet alle varianten van EAP worden ondersteund binnen NAC. Het Erasmus MC ondersteund de volgende cliënt varianten van EAP.

a. MS-PEAP , gebaseerd op windows machine en of user login authenticatie. Dit vereist een werkende koppeling gebaseerd op active directory.
b. EAP-TLS. Gebaseerd op cliënt certificaat authenticatie. Een vereiste hiervoor is een eigen ‘certificaat autoriteit’ of ook wel een Public Key Infrastructure (PKI). De systemen zijn door de eigen IT infrastructuur al voorzien van het certificaat. De NAC omgeving voorziet niet in provisioning en kan enkel het certificaat verifiëren in de authenticatie.
c. EAP-FAST, gebaseerd op loginnaam en wachtwoord voor realtime (voice/video) toepassingen. Systemen authentiseren tegen de centrale Erasmus MC user directory (Microsoft Active directory) aan.

Mac adres Authenticatie By-pass (MAB)-authenticatie

MAB authenticatie wordt alleen toegestaan wanneer het systeem geen EAP authenticatie variant ondersteund. En hiervoor toestemming is verleend door het netwerkteam en of het operationeel security team.

Om MAB authenticatie mogelijk te maken dient er een lijst in excel formaat aangeleverd te worden waarin minimaal de volgende informatie van het aan te sluiten systeem wordt aangeleverd:

a. Het MAC-adres van het te koppelen systeem;
b. De wall-outlet codering (als bedraad) van het netwerkaansluitpunt;
c. De op het systeem ingestelde hostnaam. De netwerkbeheerder behoudt zich het recht

voor om op te dragen welke hostnaam voor een systeem gehanteerd dient te worden;
d. De toepassing (korte uitleg wat het apparaat doet zodat de securityzone kan worden bepaald);

Zonder het aanleveren van de bovenstaande informatie zal er geen toegang worden verleend tot diensten op het netwerk.

Systemen welke zijn opgenomen in de NAC-database worden periodiek beoordeeld op relevantie. Netwerkbeheer verwijderd systemen geautomatiseerd uit de NAC-database op basis van de volgende criteria:

a. Hiervoor via het changeproces een verzoek is ingediend door een geautoriseerd persoon;
b. Het betreffende systeem een veiligheidsrisico vormt voor de overige gekoppelde systemen in het Erasmus MC netwerk;
c. Het systeem langer dan een periode van een half jaar aaneengesloten geen authenticatieverzoek heeft ondernomen;
d. Het systeem is opgegeven als een gestolen systeem;
e. Het systeem door Life Cycle Management is vervangen door een ander systeem en uit de configuratie database van het Erasmus MC is verwijderd.

Bij wijzigingen aan cliënt systemen dient een systeem altijd getest te worden in een NAC OTA omgeving. Leveranciers hebben hierbij een inspanningsverplichting.

2.3 Protocollen

2.3.1 Algemeen

Binnen het netwerk van het Erasmus MC wordt gebruik gemaakt van een enorme verscheidenheid aan protocollen. Dit hoofdstuk beschrijft welke eisen het Erasmus MC stelt aan het gebruik van verschillende netwerkprotocollen. Om de veiligheid en betrouwbaarheid van het netwerk te waarborgen, is het gebruik van moderne en veilige communicatieprotocollen verplicht. Daar waar mogelijk moet encryptie altijd worden toegepast binnen het toegepaste protocol. Voor encryptie methoden zie het cryptografisch beleid op KMS. Het gebruik van verouderde protocollen is niet toegestaan vanwege de potentiële veiligheidsrisico's. Hierbij wordt gedacht aan, maar niet beperkt tot de hierna beschreven protocollen.

2.3.2 Netbios

Het Netbios protocol wat in de jaren 80 werd gebruikt als voorloper van DNS mag niet meer geactiveerd worden op servers en clients die worden gekoppeld aan het Erasmus MC netwerk. Het is verplicht om DNS te gebruiken voor nameresolving binnen het Erasmus MC.

2.3.3 Transport Layer Security (TLS)

De versie van het TLS protocol moet minimaal v1.2 of hoger zijn. Gebruik van oudere versie's is niet toegestaan.

2.3.4 Lightweight Directory LDAP

Binnen het LDAP protocol dient LDAPS gebruikt te worden. Tevens dient LDAP signing ingeschakeld te zijn.

2.3.5 Server Message Block (SMB)

Alleen versie SMBv2 of hoger wordt toegestaan binnen het Erasmus MC netwerk.

2.4 Aansluitvoorwaarden voor clients[3] op het draadgebonden LAN

2.4.1 Algemeen

Dit deel van de voorwaarden heeft betrekking op het aansluiten van:

a. gebruikers-PC's, laptops;
b. netwerkprinters;
c. scanners;
d. copiers en zogenaamde 'multifunctionals;
e. IOT systemen
f. Overige niet genoemde draadgebonden systemen.

Draadgebonden systemen dienen netwerk authenticatie (802.1x) te ondersteunen en 801.1x functie dient ook te worden ingeschakeld zoals beschreven in deel 2.2.1.

Behoudens geregistreerde uitzonderingen worden dergelijke PC's en printers opgenomen in het 'gebruikersdomein *medewerker specifiek'*. Vanaf dit domein is op het niveau van het transportnetwerk toegang mogelijk tot intern/vertrouwelijke systemen en servers, waaronder het EPD. (Voor een definitie van het domeinbegrip wordt verwezen naar de 'Richtlijn Domeinen en Externe Toegang'; zie appendix, document nr 2.)

2.4.2 Netwerkaansluiting

1. Aansluitpunt: elke gebruikers-PC of netwerkprinter wordt aangesloten op **één** aansluitpunt (of op een VoIP toestel van het Erasmus MC).
2. Het te gebruiken aansluitpunt wordt **door ICT Services aangewezen**. Het aansluitpunt wordt geïdentificeerd met een code (de 'werkplekcodering').

[3] Onder clients worden verstaan: personal computers (desktops en laptops), netwerkprinters en multifunctionals. Aanname is dat draagbare/mobiele devices (smartphones, tablets) vrijwel altijd draadloos verbinding maken.

3. De **netwerkinterface** van het aangesloten systeem dient tenminste te voldoen aan **IEEE 802.3**, 1000Base-TX (1Gb p/s), auto-sensing.
4. De **netwerkinterface** van het aangesloten systeem moet om kunnen gaan met Power Over Ethernet (POE). POE wordt niet uitgeschakeld op de switchpoort om het aangesloten systeem te kunnen laten functioneren.
5. **Aansluitkabel**. Voor de verbinding tussen gebruikers-PC of netwerkprinter en aansluitpunt wordt **één door ICT Services goedgekeurde aansluitkabel** gebruikt, met een maximale lengte van **9 meter**. De specificatie van de aansluitkabel kan per locatie en gebouwdeel verschillen, zodat het juiste type kabel **voor het betreffende gebouwdeel**[4] moet worden gebruikt.
6. Het is **niet toegestaan** om:
    a. kabels te verlengen of door te koppelen;
    b. op een aansluitpunt meer dan één PC of netwerkprinter aan te sluiten;
    c. een PC op meer dan één aansluitpunt aan te sluiten;
    d. netwerkapparatuur aan te sluiten op een aansluitpunt (hubs, switches, routers, wifi-routers, gateways, inbelservers, modems, VPN gateways, etc);
    e. zelf kabelgoten te openen en/of het gotensysteem te gebruiken voor zelf-geïnstalleerde kabels, van welke aard dan ook.
    f. Een PC, laptop of printer mag slechts **met één netwerk** verbonden zijn. Binnen de muren van het Erasmus MC is dat **uitsluitend het Erasmus MC netwerk** en daarbinnen, de toegewezen netwerkzone. Aansluiting **op elk ander netwerk** (of andere netwerkzone) **is verboden**. Als ‘ander netwerk’ gelden onder andere: modemaansluitingen, telefonie en elke vorm van publieke mobiele datacommunicatie.
7. Wake-Up on Lan (WOL) wordt niet ondersteund binnen het netwerk van het Erasmus MC. Door introductie van 802.1x (NAC) in combinatie met dynamische VLAN toewijzing is het niet meer mogelijk om magic packets binnen het netwerk bij de juiste endpoints te laten uitkomen.

2.4.3 Regels ten aanzien van inrichting en gebruik

1. Het is niet toegestaan om de aangesloten PC’s zó in te richten dat deze **netwerkfuncties** vervullen, inclusief maar niet beperkt tot de functionaliteit van routers, gateways, hubs, switches, inbelservers en VPN concentrators/gateways.
2. Software die een beveiligde verbinding met een extern netwerk tot stand brengt (VPN, tunnels) mag alleen worden gebruikt als de verbinding met het interne netwerk wordt verbroken zodra de tunnel actief is.
3. Met nadruk **verboden** is het gebruik van programmatuur waarmee de eigen PC rechtstreeks vanaf Internet toegankelijk wordt gemaakt en/of vanaf Internet kan worden bestuurd. Bij twijfel dient het netwerkteam van ICT Services te worden geraadpleegd.

[4] Een actuele matrix van locatie, gebouwdelen en specificatie van het te gebruiken type aansluitkabel is te verkrijgen bij de helpdesk van ICT Services

4. Behoudens schriftelijke toestemming van ICT Services is het niet toegestaan om op gebruikers-PC's **netwerkservices** in te schakelen of aan te bieden, inclusief maar niet beperkt tot:
    a. web server;
    b. database server;
    c. file- en printer sharing;
    d. applicatieservers;
    e. remote control en remote desktop software;
    f. peer-to-peer software;
    g. DNS-, WINS- en DHCP-server software.

2.5 Aansluitvoorwaarden voor systemen op draadloze LANs

2.5.1 Algemeen

Dit deel van de voorwaarden heeft betrekking op het draadloos aansluiten van:

1. Laptops/tablets en smartphones;
2. Medische apparatuur;
3. IOT systemen;
4. VoIP telefoon toestellen;
5. Overige niet genoemde draadloze systemen.

Draadloze systemen dienen netwerk authenticatie (802.1x) te ondersteunen zoals beschreven in deel 2.2.1.

Behoudens geregistreerde uitzonderingen wordt dergelijke appratuur opgenomen in het 'gebruikersdomein *medewerker specifiek'*. Vanaf dit domein is op het niveau van het transportnetwerk toegang mogelijk tot intern/vertrouwelijke systemen en servers, waaronder het EPD. (Voor een definitie van het domeinbegrip wordt verwezen naar de 'Richtlijn Domeinen en Externe Toegang'; zie appendix, document nr 2.)

2.5.2 Structuur

1. **Gebruik van radiospectrum**: Cliënts dienen tenminste IEEE 802.11g te ondersteunen op de 2,4 GHz of 5 GHz band.
2. **SSID's**. De WLAN-infrastructuur van Erasmus MC staat maximaal 16 afzonderlijke SSID's toe, dat wil zeggen dat maximaal 16 onderling gescheiden WLAN-diensten kunnen worden gedefinieerd. Het maximaal aantal gelijktijdig uitstralende SSID's dient tot een minimum beperkt te worden. Binnen elke SSID kan met behulp van 802.1x weer onderscheid worden gemaakt naar meerdere domeinen (zoals bijvoorbeeld binnen de SSID Erasmus MC). Toewijzing van SSID's geschiedt door het netwerkteam van ICT Services.

3. Overzicht huidige geregistreerde SSIDs

ErasmusMC
Voip-messaging(-a)
Med-App
Patmon (Patiëntbewaking)
eduroam
Hotspot

2.5.3 Algemene aansluitvoorwaarden WLANs

De hier volgende aansluitvoorwaarden gelden voor **alle SSID's**:

1. **Ongeautoriseerde WLAN installaties**. Om beschikbaarheid, veiligheid en capaciteit van de gemeenschappelijke WLAN infrastructuur te kunnen garanderen is het niet toegestaan afzonderlijke WLANs op basis van IEEE 802.11 in te richten. Dat geldt zowel voor infrastructurele voorzieningen (gebaseerd op eigen access points) als voor ad hoc voorzieningen (van eindpunt naar eindpunt).
   De enige uitzondering op deze regel wordt gevormd door specifieke medische apparatuur, die op point-to-point basis gebruik kan maken van daarvoor gereserveerde kanalen.
   Niet-geautoriseerde WLAN-installaties worden door de Erasmus MC WLAN-infrastructuur gedetecteerd, waarna ICT Services maatregelen kan nemen om de niet-geautoriseerde apparatuur uit te (laten) schakelen.
2. **QoS en CoS**. Als binnen één SSID prioritering van het netwerkverkeer van bepaalde toepassingen nodig is (CoS), dan wordt daarvoor Differentiated Services (DSCP) gebruikt.
   Proces en gereedschap voor prioritering, toewijzing en beheer van bandbreedte wordt ontworpen, ingericht en beheerd door het netwerkteam van ICT Services.
3. **Encryptie**. Gebruik van WPA2-Enterprise is verplicht, behoudens door ICT Services goedgekeurde uitzonderingen per SSID.
   Als bij wijze van uitzondering WPA2-PSK wordt toegepast dan geldt hiervoor (a) dat voorafgaande registratie van de MAC-adressen van alle te gebruiken clients moet plaatsvinden en (b) dat een PSK sleutel per type apparaat uniek moet zijn.
4. **IP configuratie**. De volgende uitgangspunten gelden voor alle SSIDs:
   a. IP multicast is zeer beperkt ingericht binnen het netwerk van het Erasmus MC. Wanneer een nieuwe Multicast toepassing is gewenst zal deze nieuwe toepassing voorgelegd moeten worden aan de netwerkarchitecten. Zij bepalen nadat een concept technisch ontwerp is besproken en mogelijk testen zijn uitgevoerd of en op welk wijze de nieuwe multicast toepassing wordt geïmplementeerd;
   b. Wanneer Multicast wordt toegestaan worden multicast adresschema's toegekend door de netwerkarchitecten van het Erasmus MC. Als de apparatuur niet flexibel is om de toegewezen multicast adressen in te voeren wordt multicast niet toegestaan;

c. Toewijzing van IP-adressen verloopt via DHCP; statische IP-adressen zijn niet toegestaan (behalve voor specifiek afgestemde toepassingen in SSID 'Med-App').

2.5.4 Aansluitvoorwaarden voor clients op SSID 'ErasmusMC'

1. Deze SSID is de primaire draadloze toegang naar de **interne IT systemen** van ErasmusMC, met uitzondering van die toepassingen die hun eigen SSID hebben (zoals patiëntbewaking en telefonie).
2. **Domeinen**. Client computers in SSID 'ErasmusMC' worden via **802.1x** aan één specifiek clientdomein gekoppeld, waarbij elk domein bestaat uit een verzameling VLANs. De toewijzing van client devices aan VLANs gebeurt door de centrale authenticatie/autorisatie servers.
3. **Authenticatie en encryptie** in deze SSID is op basis van WPA2/AES in combinatie met EAP-TLS, EAP-PEAP/MSCHAPv2 of EAP/FAST.
4. Het is behoudens specifiek gemaakte afspraken niet toegestaan om met een **niet-persoonsgebonden account** toegang te verwerven tot dit SSID.
5. Er vindt in deze SSID **geen registratie** plaats van het (WLAN) MAC adres van de cliënt device.
6. Een systeem mag slechts **met één netwerk** verbonden zijn. Binnen de muren van het Erasmus MC is dat **uitsluitend het Erasmus MC netwerk** en daarbinnen, de toegewezen netwerkzone. Aansluiting **op elk ander netwerk** (of andere netwerkzone) **is verboden**. Als 'ander netwerk' gelden onder andere: modemaansluitingen, telefonie en elke vorm van publieke mobiele datacommunicatie.
7. Het is niet toegestaan om aangesloten apparatuur zó in te richten dat deze **netwerkfuncties** vervullen, inclusief maar niet beperkt tot de functionaliteit van routers, gateways, hubs, switches, inbelservers en VPN concentrators/gateways.
8. Behoudens schriftelijke toestemming van ICT Services is het niet toegestaan om op gebruikers-PC's **netwerkservices** in te schakelen of aan te bieden, inclusief maar niet beperkt tot:
   a. web server;
   b. database server;
   c. file- en printer sharing;
   d. applicatieservers;
   e. remote control en remote desktop software;
   f. peer-to-peer software;
   g. DNS-, WINS- en DHCP-server software.

2.5.5 Aansluitvoorwaarden voor de SSID's 'Voip-messaging(-a)', 'Patmon' en 'Med-App'

1. Deze SSID's zijn bedoeld:

'Voip-messaging(-a)':	voor bedrijfstelefonie en -(medisch)berichtenverkeer
'Med-App':	voor medische apparatuur
'Patmon':	voor patiëntbewaking

2. Authenticatie en encryptie vinden plaats op basis van **WPA2/PSK** (‘pre-shared key’), waarbij de volgende uitgangspunten gelden ter bescherming van het gemeenschappelijke sleutelmateriaal:
   - sleutelgegevens worden door de diensteigenaar niet ter beschikking gesteld aan enige derde, behalve beheerders die verantwoordelijk zijn voor levering en instandhouding van de diensten op deze SSID;
   - de diensteigenaar maakt een calamiteitenplan voor het geval een sleutel ‘uitlekt’;
   - devices in deze SSID’s worden ‘pre-configured’ (inclusief SSID, PSK, etc) door de diensteigenaar aan de gebruiker ter beschikking gesteld.

     Het MAC-adres van client devices wordt vooraf geregistreerd.
3. In afwijking van de algemene aansluitvoorwaarden wordt in de SSID Patmon geen DHCP gebruikt.

2.5.6 Aansluitvoorwaarden voor SSID=‘eduroam’

1. Doelgroep: medewerkers en studenten van onderwijsinstellingen en universitair medische centra die participeren in de eduroam federatie.
2. Deze SSID geeft toegang naar het Internet via de SURFnet aansluiting van Erasmus MC. Elke toegang naar interne systemen is uitgesloten.
3. Authenticatie vindt plaats op basis van 802.1x WPA2/AES (Enterprise) tegen de authenticatie/autorisatie servers van de SURFnet Federatie. De verbinding is beveiligd met PEAP/MSCHAPv2.
4. Na authenticatie worden gebruikers gekoppeld aan een afzonderlijk eduroam-VLAN (aangesloten op de VRF ‘externen’).

2.5.7 Aansluitvoorwaarden voor SSID=‘Hotspot’

1. Deze SSID is bedoeld om bezoekers en patiënten van het ErasmusMC kosteloos toegang te geven naar het **Internet**. Elke toegang naar interne systemen is uitgesloten.
2. **Onbeschermde toegang**. Toegang tot deze SSID wordt anoniem geboden, zonder registratie vooraf. Vanwege het ontbreken van authenticatie wordt geen encryptie geboden. Gebruikers moeten ervan uitgaan dat alle gegevensverkeer van/naar client devices zonder bijzondere inspanning kan worden afgeluisterd.
3. De risico’s van het gebruik van deze SSID worden uitgelegd op een portal-pagina die de gebruiker moet accorderen voordat hij/zij van het netwerk kan gebruikmaken.
4. Gebruikers worden gekoppeld aan één of meer afzonderlijke ‘hotspot’ VLANs. Uitkoppeling naar het publieke Internet loopt over een afzonderlijke firewall en (niet-SURFnet) Internet aansluiting, buiten de publieke IP-reeks van het Erasmus MC om.
5. Het is niet toegestaan om TCP/IP services aan te bieden (zoals SMTP, web, peer-to-peer services) op cliënt devices in deze SSID.

2.6 Aansluitvoorwaarden voor fysieke en virtuele servers

1. Deze aansluitvoorwaarden gelden zowel voor servers die door **ICT Services** worden ingericht en beheerd als voor servers die door **afdelingen** (‘decentraal’) worden ingericht en/of beheerd.
2. De **algemene aansluitvoorwaarden** die in 2.2 zijn vastgelegd met uitzondering van deel 2.2.1, gelden ook voor alle servers. Als regel zal echter voor een server een of meerdere vast(e) IP-adres(sen) worden gereserveerd.
3. Behoudens schriftelijke toestemming van ICT Services is het verboden om server-programmatuur voor de **volgende infrastructurele diensten** te activeren:
    1. Domain Name System (DNS)
    2. Dynamic Host Configuration Protocol (DHCP) en/of Boot Protocol (BOOTP)
    3. Windows Internet Naming Service (WINS)
    4. Lightweight Directory Access Protocol (LDAP)
    5. Microsoft Active Directory Service (AD)

    ICT Services is verantwoordelijk voor het inrichten en beheren van centrale faciliteiten voor bovengenoemde services.
4. Fysieke servers worden geplaatst in de datacenters van ICT Services. Wanneer dit in een uitzonderingssituatie om operationele reden niet mogelijk is, wordt de server geplaatst in een ruimte die **niet openbaar toegankelijk** is voor Erasmus MC-medewerkers. De betreffende ruimte wordt door de lokale beheerder afgesloten als hij/zij daar niet aanwezig is. De lokale beheerder neemt maatregelen om te voorkomen dat derden zich onbevoegd toegang kunnen verschaffen tot de server.
5. **Server-hardware** geplaatst in door ICT Services beheerde datacenters dient gemonteerd te kunnen worden in een 19” rack.
6. Elke server draagt één of meer informatiesystemen en/of informatieverzamelingen. **Classificatie** hiervan is verplicht conform het beveiligingsbeleid van het Erasmus MC. Op basis van deze classificatie wordt elke server in **één beveiligingsdomein** geplaatst. (Zie literatuurlijst, document 4: “Richtlijn Classificatie van bedrijfsprocessen, informatiesystemen en informatie”.)
7. In afwijking van (f) kunnen de **beheers- of console-poorten** van een server in het infrastructuur-domein worden opgenomen.
8. De server operating system versie dient altijd afgestemd te worden met het serverbeheerteam.
9. Servers worden voorzien van de bij het Erasmus MC in gebruik zijnde anti virus/spam software welke centraal door het Erasmus MC wordt beheert.
10. Middels een centrale management tool beheert door het serverbeheerteam van het Erasmus MC, worden servers op reguliere basis voorzien van patches.
11. Servers worden dagelijks geback-upt.

Als andere afdelingen dan ICT Services, servers hebben geplaatst in een door ICT Services beheerde SER, MER of datacenter, dan zal ICT Services op aanvraag van de afdeling zorgdragen voor toegang tot een passend gedeelte van het infrastructuur-domein. Dit met als

doel dat de eigen beheerders van de afdeling toegang hebben tot de beheerspoorten van de eigen servers.

2.7 Aansluitvoorwaarden voor externe toegang

Ten behoeve van toegang van buitenaf naar systemen binnen de muren van het Erasmus MC is het **verplicht** gebruik te maken van de **centrale voorzieningen** die door ICT Services worden aangeboden en beheerd.

Voor meer informatie ten aanzien van de **beveiligingsmaatregelen**, procedures en gedragsregels die van toepassing zijn bij externe toegang wordt verwezen naar de ‘Richtlijn Domeinen en Externe Toegang’ (zie appendix, document nr. 2).

3 Toezicht op naleven van de aansluitvoorwaarden en sancties

3.1 Toezichthouder

Medewerkers van ICT Services , die in opdracht van de manager ICT Services de taak hebben toezicht te houden op het gebruik van de geboden faciliteiten, zijn in het kader daarvan gerechtigd instructies of aanwijzingen te geven en/of sancties op te leggen.

3.2 Overtreding aansluitvoorwaarden

1. Bij constatering van overtreding van de in deze aansluitvoorwaarden opgenomen regels en voorwaarden door een medewerker of een afdeling van het Erasmus kunnen sancties opgelegd worden zoals beschreven in de Gedragscode voor het gebruik van computerfaciliteiten van het Erasmus MC

2. Bij constatering van overtreding van de in deze aansluitvoorwaarden opgenomen regels en voorwaarden kan het Erasmus MC de desbetreffende externe medewerker en/of organisatie een sanctie opleggen met betrekking tot het doelmatig, c.q. rechtmatig gebruik van de computerfaciliteiten. De uitvoering van deze sanctie is een gemandateerde bevoegdheid van de manager ICT Services. Deze sanctie kan onder andere bestaan uit het uitsluiten van de apparatuur van de externe medewerker en/of organisatie van toegang tot Erasmus MC-netwerk voor(on)bepaalde tijd.

3. Wanneer een externe medewerker en/of organisatie één of meer van de uit deze aansluitvoorwaarden voortvloeiende verplichtingen schendt, zal het Erasmus MC de organisatie aansprakelijk stellen voor alle schade die voortvloeit uit deze overtreding. Bovendien heeft ICT Services het recht de externe medewerker en/of organisatie van toegang tot Erasmus MC-netwerk voor(on)bepaalde tijd uit te sluiten.

3.3 Aansprakelijkheid

De gebruiker die schade veroorzaakt door het niet naleven van deze aansluitvoorwaarden is voor deze schade aansprakelijk. Hieronder valt ook schade die ontstaan is door malware.

Onder schade wordt verstaan feitelijke schade aan het Erasmus MC-netwerk, maar ook gevolgschade bij eventuele andere gebruikers als gevolg van het niet (goed) functioneren van het Erasmus MC-netwerk.

4 Appendix A: Literatuurlijst

1. Gedragscode voor het gebruik van computerfaciliteiten
2. TOE-R-1, Richtlijn Domeinen en Externe Toegang
3. I-SO-RP-FYS-JWS Richtlijn fysieke toegangsverlening ruimten
4. CLA-R-1, Richtlijn Classificatie van bedrijfsprocessen, informatiesystemen en informatie,

Bovenstaande documenten, behalve de gedragscode, zijn in beheer bij de Chief Information Security Officer (CISO) en de IT Security Officer van het Erasmus MC. De gedragscode is in beheer bij HR.

5 Appendix B: Verklarende afkortingen en woordenlijst

Woord	Verklaring
Hostname/Host	Naam van een apparaat op het netwerk. Ook wel DNS-naam genoemd.
IP	De IP in IP-adres staat voor Internet Protocol. Het is een techniek die gebruikt wordt om computers in een netwerk met elkaar te laten communiceren. De meest gebruikte toepassing is het internet. In een IP-netwerk krijgt elke computer een unieke code toegewezen (vergelijk het met een telefoonnummer).
IP-Adres	Het adres waarmee een systeem op het netwerk communiceert met andere aan het netwerk aangesloten systemen.
MAC -adres	Een MAC-adres is een uniek identificatienummer van een systeem wat aan het netwerk wordt verbonden. Dit unieke identificatienummer is hard 'ingebrand' in de netwerkkaart van een systeem. De notatie van een MAC-adres is in hexadecimaal formaat. De eerste 6 karakters van een MAC-adres is een fabrikant aanduiding.
DNS	DNS staat voor Domain Name Service. Deze netwerkservice zorgt er voor dat IP-adressen worden vertaald naar een vriendelijkere naam op het netwerk. Een DNS-server heeft een database waarin onder andere IP-adres en naam in een record zijn opgeslagen. Binnen het netwerk kan aan de DNS-server worden gevraagd om een IP-adres op te zoeken behorende bij een naam.
DHCP	DHCP staat voor Dynamic Host Configuration Protocol. Deze netwerkservice draagt zorg voor het uitdelen van IP-adressen aan systemen die zich aanmelden op het netwerk en om een IP-adres vragen.
NAC	Network Access Control – Een functionaliteit die voorziet in netwerk toegangscontrole. Zonder NAC zou het netwerk een open karakter hebben. Doormiddel van NAC kan alleen geautoriseerde apparatuur worden ontsloten worden op het netwerk. Naast netwerk toegangscontrole biedt NAC ook inzicht in de aangesloten netwerkapparatuur.
LAN	LAN staat voor Local Area Network. Het Local Area Network is het bekabelde netwerk. Ieder systeem dat met een patchkabel aan het netwerk wordt verbonden, is verbonden aan het LAN.
WLAN	WLAN staat voor Wireless Local Area Network. Ook wel genoemd draadloos/wifi netwerk.
WOL	Wakeup On LAN. Dit protocol zorgt er voor dat middels een broadcast over het netwerk op een specifieke poort een MAC adres kan worden aangeroepen. Dit met als doel een systeem wat in sluimer mode staat kan worden ingeschakeld door het betreffende broadcast packet
EAP	EAP staat voor Extensible Authentication Protocol. Dit is een raamwerk voor het gestandaardiseerd kunnen authentiseren van een systeem aan het LAN en WLAN.
PC	Personal Computer

VPN	VPN staat voor Virtual Private Network. Met een VPN kan een beveiligde verbinding worden opgezet tussen twee partijen. Er wordt als het ware een soort beveiligde tunnel gemaakt waardoor netwerkverkeer loopt. Door gebruik te maken van een VPN kan de communicatie tussen twee partijen wel worden onderschept maar qua inhoud niet worden ontcijferd.
VOIP	VOIP staat voor Voice Over IP. Met een systeem wat kan communiceren op basis van VOIP kunnen telefoongesprekken worden gevoerd over een IP-netwerk
Access	De access betreft de systemen aan de werkplek zijde van het netwerk.
Core	De core is het systeem wat in het hart van het netwerk staat. Dit systeem maakt de beslissingen welke IP-pakketten over welke verbindingen worden gerouteerd.
FQDN	Een Fully Qualified Domain Name (FQDN) is een geheel uitgeschreven netwerknaam van een systeem. Meestal bestaat de FQDN uit de hostname plus een domeinnaam.
Active Directory	Een Active Directory is een database waarin alle door het bedrijf gebruikte identiteiten worden beheerd.
MAB	Mac-address Authentication By-pass. Middels deze vorm van authenticatie kan een systeem worden toegelaten op het netwerk door het MAC adres te registreren in de NAC database.
TLS	Transport Layer Security (TLS) is een cryptografisch protocol dat is ontworpen om communicatiebeveiliging te bieden via een computernetwerk.
LDAP	Lightweight Directory Access Protocol (LDAP) is een lichtgewicht versie van het Directory Access Protocol dat deel uitmaakt van X.500, een standaard voor directoryservices in een netwerk. LDAP wordt als lichtgewicht beschouwd omdat het minder code gebruikt dan andere protocollen. Een directory vertelt de gebruiker waar in het netwerk iets zich bevindt.
SMB	Server Message Block (SMB) is een communicatieprotocol dat wordt gebruikt om bestanden, printers, seriële poorten en diverse communicatie tussen knooppunten in een netwerk te delen.