



Document	Aansluitvoorwaarden Erasmus MC-netwerk
Versie	8.0
Datum	22 januari 2015
Opsteller	Paul Driever, Pieter van Dorp, Lars Hameeteman, Peter Kleynjan
Beheerder	Paul Driever
Opdrachtgever	Nico Drost
Ter goedkeuring aan	Managementteam Service Organisatie

Aansluitvoorwaarden Erasmus MC-netwerk

Inhoudsopgave

1 Algemeen	3
1.1 Doel	3
1.2 Vaststelling en wijziging	3
1.2.1 Aansluitvoorwaarden	3
1.2.2 Uitzonderingen	3
1.3 Publicatie	3
2 Aansluitvoorwaarden netwerkinfrastructuur	4
2.1 Leeswijzer	4
2.2 Algemene aansluitvoorwaarden	5
2.3 Aansluitvoorwaarden voor clients op het draadgebonden LAN	6
2.3.1 Algemeen	6
2.3.2 Netwerkaansluiting	7
2.3.3 Regels ten aanzien van inrichting en gebruik	7
2.4 Aansluitvoorwaarden voor systemen op draadloze LANs	8
2.4.1 Structuur	8
2.4.2 Algemene aansluitvoorwaarden WLANs	9
2.4.3 Aansluitvoorwaarden voor clients op SSID 'ErasmusMC'	9
2.4.4 Aansluitvoorwaarden voor de SSID's 'Voip-messaging-a', 'Patmon' en 'Med-app'	10
2.4.5 Aansluitvoorwaarden voor SSID='eduroam'	11
2.4.6 Aansluitvoorwaarden voor SSID='Hotspot'	11
2.5 Aansluitvoorwaarden voor servers	12
2.6 Aansluitvoorwaarden voor externe toegang	13
3 Toezicht op naleven van de aansluitvoorwaarden en sancties	14
3.1 Toezichthouder	14
3.2 Sanctie	14
3.3 Aansprakelijkheid	15
4 Appendix: Literatuurlijst	16

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 Service Organisatie 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 Service Organisatie een voorstel hiertoe worden gedaan door de business manager van IT Operations.

1.2.2 Uitzonderingen

Over uitzonderingen op de in dit stuk gestelde voorwaarden beslist de leiding van IT Operations 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 aansluitvoorwaarden voor client PC's op het draadgebonden LAN;
- 2.4 aansluitvoorwaarden voor systemen op draadloze LANs;
- 2.5 aansluitvoorwaarden voor servers;
- 2.6 aansluitvoorwaarden voor externe toegang.

Deel 2.2 beschrijft aansluitvoorwaarden die voor **alle systemen en alle domeinen** gelden.

Het onderscheid tussen de delen 2.3 / 2.4 en anderzijds deel 2.5 rust op de domeinindeling die is ingesteld ter compartimentering van de netwerk-infrastructuur¹:

- * 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.

Het netwerk van ErasmusMC is onderverdeeld in **netwerkkzones** (geïmplementeerd als zgn. VRF's), waarvan de belangrijkste zijn:

- 1 intern
- 2 student
- 3 externen
- 4 hotspot
- 5 patiëntbewaking
- 6 isolatie

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

a **Antivirus**-bescherming.

Elk systeem moet zijn voorzien van programmatuur die de PC (en alle daarop geïnstalleerde software en bestanden) beschermt tegen besmetting door virussen en andere vormen van kwaadaardige programmatuur. De gebruiker c.q. eigenaar van de pc is verplicht deze programmatuur (en eventueel bijbehorende gegevensbestanden) up-to-date en actief² te (laten) houden.

Deze eis geldt niet voor systemen in de netwerkkzones 'hotspot' (4) en 'patiëntbewaking' (5).

b **Software-licenties.**

Toegestaan is alleen installatie en gebruik van software waarvoor een licentieovereenkomst aanwezig is, hetzij bij IT Operations, hetzij op de afdeling zelf.

Deze eis geldt niet voor systemen in de netwerkkzone 'hotspot' (4).

c **TCP/IP.** Alle aangesloten systemen maken uitsluitend gebruik van IP om toegang te krijgen tot de logische netwerk-infrastructuur.

² onder '**actief gehouden**' wordt verstaan dat de programmatuur scant op virussen en andere vormen van kwaadaardige programmatuur

- bij het opstarten van de pc
- bij het lezen van externe gegevensbronnen
- bij het openen van bestanden op externe gegevensbronnen
- bij het downloaden van bestanden van Internet/Intranet of andere externe netwerken waarmee verbinding is opgebouwd (zoals toegestaan binnen deze aansluitvoorwaarden).

- d Om brede connectiviteit te waarborgen beheert IT Operations centrale **DHCP- en DNS servers**. Het gebruik hiervan is verplicht.

Dit betekent:

- voor DNS wordt uitsluitend gebruik gemaakt van de centrale servers;
- het IP-adres wordt met behulp van '**automatisch opvragen**' verkregen, dat wil zeggen dat het adres dynamisch toegewezen wordt door de centrale DHCP servers.

In afwijking van het bovenstaande kan bij IT Operations een (gemotiveerde) aanvraag worden gedaan voor een **vast IP adres**; een dergelijk vast IP adres kan **alleen** door het netwerkteam van IT Operations worden toegewezen.

Deze eis geldt niet voor systemen in de netwerkzone 'patiëntbewaking' (5).

- e Software dient zo veel mogelijk zó geconfigureerd te worden dat DNS host names worden gebruikt in plaats van IP-adressen.
- f Applicatiesoftware die 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 IT Operations.
- g 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 IT Operations worden gebruikt ten behoeve van het beheer van PC's.
- h 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").

Deze eis geldt niet voor systemen in de netwerkzone 'hotspot' (4).

2.3 Aansluitvoorwaarden voor clients³ op het draadgebonden LAN

2.3.1 Algemeen

Dit deel van de voorwaarden heeft betrekking op het aansluiten van **gebruikers-PC's**, laptops en netwerkprinters (inclusief scanners, copiers en zogenaamde 'multifunctionals') op het Erasmus MC-netwerk via de 'draadgebonden' LAN-infrastructuur.

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.)

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.

2.3.2 Netwerkaansluiting

- a **Aansluitpunt:** elke gebruikers-PC of netwerkprinter wordt aangesloten op **één** aansluitpunt.
- b Het te gebruiken aansluitpunt wordt **door IT Operations aangewezen**. Het aansluitpunt wordt geïdentificeerd met een code (de 'werkplekcodering').
- c De **interface** van PC of netwerkprinter dient te voldoen aan **IEEE 802.3**, 10Base-T/100Base-TX/1000Base-TX, auto-sensing.
- d **Aansluitkabel.** Voor de verbinding tussen gebruikers-PC of netwerkprinter en aansluitpunt wordt **één door IT Operations 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 gebouwdeel⁴** moet worden gebruikt.

- e Het is **niet toegestaan** om:
 - kabels te verlengen of door te koppelen;
 - op een aansluitpunt meer dan één PC of netwerkprinter aan te sluiten;
 - een PC op meer dan één aansluitpunt aan te sluiten;
 - netwerkapparatuur aan te sluiten op een aansluitpunt (hubs, switches, routers, gateways, inbelservers, modems, VPN gateways, etc);
 - 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.

2.3.3 Regels ten aanzien van inrichting en gebruik

- a 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.

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.

Met nadruk **verboden** is het gebruik van programmatuur waarmee de eigen PC van buitenaf toegankelijk wordt gemaakt en/of van buitenaf kan worden bestuurd.

Bij twijfel dient het netwerkteam van IT Operations 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 IT Operations

- b Behoudens schriftelijke toestemming van IT Operations is het niet toegestaan om op gebruikers-PC's **netwerkservices** in te schakelen of aan te bieden, inclusief maar niet beperkt tot:

- web server;
- database server;
- file- en printer sharing;
- applicatieservers;
- remote control en remote desktop software;
- peer-to-peer software;
- DNS-, WINS- en DHCP-server software.

2.4 Aansluitvoorwaarden voor systemen op draadloze LANs

2.4.1 Structuur

a **Gebruik van radiospectrum:**

- 1 **802.11a** (5 GHz) is gereserveerd voor tijdkritische toepassingen zoals telefonie;
- 2 Overige toepassingen maken gebruik van **802.11g en -n**.

- b **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.

Binnen elke SSID kan met behulp van 802.1x weer onderscheid worden gemaakt naar meerdere domeinen (zoals bijvoorbeeld binnen de SSID ErasmusMC).

Toewijzing van SSID's geschiedt door het netwerkteam van IT Operations.

c **Overzicht huidige geregistreerde SSIDs**

	802.11a	802.11g/n
ErasmusMC	X	V
Voip-messaging-a	V	X
Med-app	X	V
Patmon (Patiëntbewaking)	V ⁵	V
eduroam	X	V
Hotspot	X	V

V = toegestaan, X = niet toegestaan

⁵ Gebruik van 802.11g voor patiëntbewaking is toegestaan, maar 802.11a heeft de voorkeur

2.4.2 Algemene aansluitvoorwaarden WLANs

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

- a **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 IT Operations maatregelen kan nemen om de niet-geautoriseerde apparatuur uit te (laten) schakelen.

- b **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 IT Operations.

- c **Encryptie.** Gebruik van WPA2 is verplicht, behoudens door IT Operations goedgekeurde uitzonderingen per SSID.

Als bij wijze van uitzondering 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 SSID uniek moet zijn.

- d **IP configuratie.** De volgende uitgangspunten gelden voor alle SSIDs:

- IP multicast is vooralsnog niet toegestaan;
- toewijzing van IP-adressen verloopt via DHCP; statische IP-adressen zijn niet toegestaan.

2.4.3 Aansluitvoorwaarden voor clients op SSID 'ErasmusMC'

- a 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).
- b **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 radius servers.
- c Een apparaat of gebruiker die door inrichting of gedrag een mogelijk hoger risico met zich meebrengt wordt als zodanig geïdentificeerd en geregistreerd en daarna via de radius servers in een apart **quarantaine-VLAN** gekoppeld.

- d **Authenticatie en encryptie** in deze SSID is op basis van WPA2/AES in combinatie met EAP-TTLS of EAP-PEAP/MSCHAPv2.
- e Het is niet toegestaan om met een **niet-persoonsgebonden account** toegang te verwerven tot dit SSID.
- f Er vindt in deze SSID **geen registratie** vooraf plaats van het (WLAN) MAC adres van de client device.
- g 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.
- h 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.
- i Behoudens schriftelijke toestemming van IT Operations is het niet toegestaan om op gebruikers-PC's **netwerkservices** in te schakelen of aan te bieden, inclusief maar niet beperkt tot:
 - web server;
 - database server;
 - file- en printer sharing;
 - applicatieservers;
 - remote control en remote desktop software;
 - peer-to-peer software;
 - DNS-, WINS- en DHCP-server software.

2.4.4 Aansluitvoorwaarden voor de SSID's 'Voip-messaging-a', 'Patmon' en 'Med-app'

- a Deze SSID's zijn bedoeld:
 - 'Voip-messaging-a': voor bedrijfstelefonie en –berichtenverkeer
 - 'Med-app': voor medische apparatuur
 - 'Patmon': voor patiëntbewaking
- b 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 levering en instandhouding voor de diensten op deze SSID;
 - de diensteigenaar maakt een contingency plan 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.

- c In afwijking van de algemene aansluitvoorwaarden wordt in de SSID Patmon geen DHCP gebruikt.

2.4.5 Aansluitvoorwaarden voor SSID='eduroam'

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

2.4.6 Aansluitvoorwaarden voor SSID='Hotspot'

- a 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.
- b **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.

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.
- c Gebruikers worden gekoppeld aan één of meer afzonderlijke 'hotspot' VLANs. Uitkoppeling naar het publieke Internet loopt over een afzonderlijke firewall en (non-SURFnet) Internet aansluiting, buiten de publieke IP-reeks van het ErasmusMC om.
- d Het is niet toegestaan om TCP/IP services aan te bieden (zoals SMTP, web, peer-to-peer services) op client devices in deze SSID.

2.5 Aansluitvoorwaarden voor servers

- a Deze aansluitvoorwaarden gelden zowel voor servers die door **IT Operations** worden ingericht en beheerd als voor servers die door **afdelingen** ('decentraal') worden ingericht en/of beheerd.
- b De **algemene aansluitvoorwaarden** die in 2.2 zijn vastgelegd gelden ook voor alle servers. Als regel zal echter voor een server een vast IP-adres worden gereserveerd.
- c Behoudens schriftelijke toestemming van IT Operations is het verboden om server-programmatuur voor de **volgende infrastructurele diensten** te activeren:
 - Domain Name System (DNS)
 - Dynamic Host Configuration Protocol (DHCP) en/of Boot Protocol (BOOTP)
 - Windows Internet Naming Service (WINS)
 - Lightweight Directory Access Protocol (LDAP)
 - Microsoft Active Directory Service (AD)IT Operations is verantwoordelijk voor het inrichten en beheren van centrale faciliteiten voor bovengenoemde services.
- d Een server wordt geplaatst in één van de **centrale computerruimten** van IT Operations. 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.
- e **Server-hardware** geplaatst in door IT Operations beheerde SER-, MER- of Computerruimten dient 19" rack mounted te zijn.
- f Elke server draagt één of meer informatiesystemen en/of informatieverzamelingen. **Classificatie** hiervan is verplicht conform het beveiligingsbeleid van 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".)
- g In afwijking van (f) kunnen de **beheers- of console-poorten** van een server in het infrastructuur-domein worden opgenomen.

Als andere afdelingen dan de IT Operations servers hebben geplaatst in door IT Operations beheerde SER-, MER- of Computerruimten, dan zal IT Operations 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.

2.6 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 IT Operations 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 IT Operations, die in opdracht van de business manager IT Operations 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. Ditzelfde geldt voor leden van het CERT.

3.2 Sanctie

In geval van overtreding van de in deze aansluitvoorwaarden opgenomen regels en voorwaarden door een medewerker of een afdeling van het Erasmus MC gelden de volgende bepalingen:

- a. Bij constatering van misbruik van computerfaciliteiten of het gebruik in strijd met de regelgeving of wettelijke bepalingen door een medewerker, waaronder de Gedragscode voor het gebruik van computerfaciliteiten van het Erasmus MC, kan de Raad van Bestuur een **medewerker** een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiestelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de CAO Universitaire Medische Centra. Bovendien heeft IT Operations het recht de gebruiker van toegang tot Erasmus MC-netwerk voor (on)bepaalde tijd uit te sluiten.
- b. Bij constatering van misbruik van computerfaciliteiten of het gebruik in strijd met de regelgeving of wettelijke bepalingen door een afdeling, kan de Raad van Bestuur de desbetreffende **afdeling** 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 business manager IT Operations. Deze sanctie kan onder andere bestaan uit het uitsluiten van de apparatuur van de afdeling van toegang tot Erasmus MC-netwerk voor (on)bepaalde tijd.
- c. Tegen het instellen van de sancties of andere acties op grond van deze aansluitvoorwaarden kan de gebruiker en/of de afdeling bezwaar maken volgende de bezwarenprocedure van het Erasmus MC en hetgeen hierover is vastgelegd in de Algemene Wet Bestuursrecht (Awb)

In geval van overtreding van de in deze aansluitvoorwaarden opgenomen regels en voorwaarden door een externe medewerker of organisatie gelden de volgende bepalingen:

- a. 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 business manager IT Operations. 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.
- b. 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 IT Operations 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 de verspreiding van kwaadaardige programmatuur, waaronder virussen, als gevolg van het niet up-to-date en/of actief hebben van virusprotectieprogrammatuur.

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: Literatuurlijst

1. Gedragscode voor het gebruik van computerfaciliteiten van het Erasmus MC, versie 1.1, 14 november 2005
2. TOE-R-1, Richtlijn Domeinen en Externe Toegang, versie 1.1, 10 februari 2006
3. FYS-R-1, Richtlijn fysieke toegangverlening ruimten IT Operations, versie 1.8, 8 januari 2014
4. CLA-R-1, Richtlijn Classificatie van bedrijfsprocessen, informatiesystemen en informatie, versie 2.0, december 2013.

Bovenstaande documenten zijn in beheer bij de Chief Information Security Officer (CISO) en de IT Security Officer van het Erasmus MC.