Documentgegevens

Titel	Reglement omgang met Informatie en IT middelen bij MUMC+
Werkgebied	Informatiebeveiliging
Trefwoorden	e-mail, email, ICT, computer, internet, IT

Dit document is alleen geldig op de aangegeven printdatum, tenzij de volgende gegevens zijn ingevuld:	
Naam documentbeheerder:	.....
Paraaf:	.....
Tst. nr:	.....
Geldig t/m (datum):	.....

Samenvatting

Dit document is dé MUMC+ leidraad voor o.a. het gebruik van informatie en IT-middelen. Naar eventuele aanvullende regelgeving wordt verwezen. Dit document is zonder uitzondering van toepassing op iedere gebruiker van informatie- en IT-middelen in het MUMC+.

NB: Dit document vervangt bij publicatie de volgende Odin documenten:
- *E-mail: gebruik in het azM*
- *Internet: gebruik in het azM*
- *(Computer) werkplek in het azM,*
- *ICT middelen: aanvragen door gebruiker*

Beleid en doelstellingen

Reglement omgang met Informatie en IT middelen bij MUMC+

17 maart 2016	De datum waarop dit reglement is vastgesteld door de RvB van de instelling.
1 mei 2016	De datum waarop dit reglement in werking treedt binnen de instelling.

Doel

Het doel van dit reglement is duidelijk maken wat het MUMC+ verstaat onder aanvaardbaar en toelaatbaar gebruik van haar IT-middelen en de opgebouwde informatie binnen MUMC+ alsmede het tegengaan van misbruik dan wel oneigenlijk gebruik.

Definities

1. Tot *gebruikers* worden gerekend: medewerkers die, betaald of onbetaald, in, voor of namens MUMC+ werkzaamheden verrichten, daaronder mede begrepen in of voor MUMC+ werkzame medewerkers van en met MUMC+ verbonden organisaties, in het kader van overeenkomsten tussen MUMC+ en andere bedrijven en organisaties in het MUMC+ werkzame personen, gedetacheerden, stagiaires en coassistenten, en onderwijsvolgenden die bij of middels MUMC+ onderwijs volgen, daar onder mede begrepen het afleggen van tentamens en examens.
2. Een *werkplek* omvat de door het Stafdirectoraat MIT aan werknemers beschikbaar gestelde apparatuur zoals een PC, laptop, tablet-PC, PDA, smartphone, telefoon, GSM. In gegeven gevallen kunnen deze gekoppeld zijn aan medische apparatuur: medische werkplek. Medische werkplekken zijn computerwerkplekken met specifieke software voor de aansturing van medische onderzoeks- of behandelingsapparatuur.

3. *BYOD* (Bring Your Own Device) het fenomeen waarbij een organisatie (het azM) het voor haar werknemers mogelijk maakt hun privé-mobiele apparaten, zoals smartphones, tablets of laptops, voor het werk te gebruiken en te verbinden met het bedrijfsnetwerk en een beperkte toegang tot generieke toepassingen. Wanneer een dergelijk device gebruikt wordt voor benoemde toegang gelden dezelfde regels als voor een azM werkplek.
4. Onder *IT-middelen* verstaan we zowel de computerwerkplekken als ook de randapparatuur (bv. monitoren, printers, scanners, toetsenborden), evenals programmatuur en datadragers.
5. Als *datadragers* kennen we onder andere externe harddisks, Cd-roms, Dvd's, USB-sticks, diskettes, memorycards.
6. Bedrijfs- en patiëntinformatie op de werkplek wordt geleverd door *software*, dit bijvoorbeeld in de vorm van portals, applicaties, app's -.
7. Onder *illegale* software wordt verstaan software waarvoor ten onrechte geen licentie- of auteursrechten worden betaald. Een bijzonder geval van illegaal gebruik kan zijn het gebruik van *freeware* voor zakelijke toepassingen. Verifieer daartoe de betreffende gebruiksvoorwaarden. Onder *freeware* wordt verstaan software waarvoor geen licentiekosten hoeven te worden betaald en veelal bedoeld zijn voor persoonlijk gebruik.
8. Onder *malafide software* wordt software van kwaadaardige aard verstaan, bijv. virussen en spionage software (spyware).
9. Corporate Security Officer (CSO, ook wel Chief Security Officer genoemd)): de hoogste MUMC+ functionaris die specifiek verantwoordelijk is voor (toezicht op) informatiebeveiliging en privacybescherming.
10. Computer Security Incident Response Team (CSIRT): het MUMC+ team (MUMC-CSIRT) dat binnen de instelling de eerste (technische) response verzorgt bij beveiligingsincidenten.
11. Een lid van de MUMC-CSIRT: een functionaris die gericht onderzoek kan en mag doen naar mogelijke overtredingen.
12. De gemandateerd leidinggevende is de directe lijnmanager van de medewerker.
13. Onder standaard assortiment wordt verstaan het geheel van IT-producten die vanuit MUMC is getoetst, goedgekeurd en vanuit MIT geleverd kan worden.

Artikel 1 Algemene bepalingen

Lid:

1. Gebruik van informatie- en communicatietechnologie- zoals computers, netwerk en aanverwante faciliteiten als applicaties, internet, e-mail (hierna: IT-middelen) binnen, bij, vanwege of voor MUMC+ is onderworpen aan de regels zoals onder meer in dit reglement beschreven.
2. De gebruiker is verplicht zich zodanig te gedragen dat de informatievoorziening niet wordt bedreigd, belemmerd of verstoord, gevoelige gegevens (waaronder persoonsgegevens) niet worden geopenbaard aan anderen, de wet niet wordt overtreden en de reputatie van MUMC+ niet wordt geschonden.

Artikel 2 Toegangsverlening en bevoegdheden

Lid:

1. De door de Raad van Bestuur gemandateerde leidinggevende kan een medewerker ter uitvoering van diens werkzaamheden toegang (doen) laten verlenen tot de verschillende onderdelen van de informatievoorziening van MUMC+ en daarmee tot het gebruik van ICT-middelen (ODIN 030912).
2. Bevoegdheden ten aanzien van het gebruik van IT-middelen, toegang tot en het bewerken van data worden slechts verleend aan een gebruiker waarvan ten allereerste de identiteit is vastgesteld middels een door de Wet op de identificatieplicht aangewezen identiteitsbewijs (identificatie- en verificatieplicht van het MUMC+), en ten tweede de vereiste rechten zijn vastgesteld door de leidinggevende en de systeemeigenaar.
3. Wachtwoorden zijn een belangrijk middel om de persoonlijk geoorloofde toegang tot de MUMC+ informatiesystemen te verschaffen en te borgen. De aspecten vertrouwelijkheid, integriteit en beschikbaarheid van de informatie en de systemen staan voorop (ODIN 004093).
4. De toegang tot de systemen van het MUMC+ vanuit externe locaties via internet, is uitsluitend toegestaan via een beveiligde VPN-verbinding. Voor de toegang tot persoonsgegevens (bv. patiënt- of medewerkersgegevens) en bedrijfsgegevens is naast de VPN-toegang een

verhoogde authenticatiesterkte vereist (minimaal 2 factor: met iets wat je weet en iets wat je hebt bv. een *token*).
5. Aan de toegang tot ruimtes zijn beperkingen opgelegd zoals bijvoorbeeld rekencentra (MIT), laboratoria, bestuursgebouw, etc. Goedkeuring van de toegangsverlening per smartcard vindt plaats door de verantwoordelijke manager van de ruimte. De gebruiker vraagt de toegang aan bij het loket Facilitair Bedrijf.

Artikel 3 Basisregels voor gebruik
Lid:

Algemeen
1. In het kader van het vervullen van zijn of haar functie worden aan de gebruiker IT-middelen beschikbaar gesteld. De middelen die deel uitmaken van de informatievoorziening van het MUMC+ zijn ook eigendom van de organisatie. De gebruiker is verantwoordelijk voor correct en legaal gebruik van de beschikbaar gestelde middelen.
2. Aanschaf, ter beschikking stelling en buiten gebruikstelling van IT-middelen vindt plaats door of onder regie van het Stafdirectoraat MIT. Dit leidt tot hogere kwaliteit van de informatievoorziening, betere ondersteuning en adequaat beheer van licenties. IT-middelen die niet tot het standaard assortiment behoren kunnen de bedrijfsvoering in gevaar brengen. Het beleid omtrent IT-middelen is vastgelegd in het document MUMC beleid IT-middelen (ODIN 005415).
3. De medewerker die uit dienst treedt (of van functie wisselt), draagt zorg voor het inleveren van de in bruikleen verstrekte (IT) bedrijfsmiddelen conform de procedure “Uitdiensttredingsprocedure, werkinstructie”, ODIN document nummer 031379. Indien de bedrijfsmiddelen niet op de laatste werkdag zijn ingeleverd kunnen er kosten in rekening worden gebracht. Daarnaast is het noodzakelijk (als verder vermeld in bovenstaande procedure) dat alle nog openstaande werkprocessen in de diverse informatiesystemen, correct worden afgesloten of binnen SAP aan collega’s worden gedelegeerd zodat deze de werkzaamheden kunnen afronden.

Aanschaf
4. Elke gebruiker kan een aanvraag voor standaard IT-middelen indienen (ODIN 004091) middels een aanvraag via de afdelingsverantwoordelijke. Aanschaf van niet via MIT als standaard leverbare middelen dient te worden besproken met de betreffende MIT Information Engineer.

Gebruik
5. Het gebruik van IT-middelen is aan een gebruiker slechts toegelaten voor de uitvoering van diens werkzaamheden.
6. De gebruiker is gehouden elk onderdeel van de IT-middelen van het MUMC+ te gebruiken overeenkomstig de voor het onderdeel geldende instructies.
7. De gebruiker dient op de hoogte te zijn van de algemene beveiligingsregels en de specifieke beveiligingsregels die voor het betreffende (onderdeel van het) IT-middel gelden.
8. Identificatiekenmerken van IT-middelen mogen niet worden verwijderd of onbruikbaar worden gemaakt.
9. De gebruiker is zelf verantwoordelijk voor veilige omgang met gegevens, in het bijzonder persoonsgegevens, en is verplicht zorg te dragen voor het veilig opslaan, veilig verzenden en veilig vernietigen van gegevens. De Raad van Bestuur kan hier nadere regels aan stellen; deze zijn opgenomen als bijlage A bij dit reglement. De omgang met persoonsgegevens vindt zijn grondslag in de Wet bescherming persoonsgegevens (WBP). Onzorgvuldig gebruik is hierin strafbaar gesteld.
10. Voor alle gebruikers van de internet en email faciliteit geldt een gedragscode als vastgelegd in document *Gedragscode voor het gebruik van internet en e-mail voor azM medewerkers* (ODIN 022408).
11. Elke gebruiker wordt voorzien van een unieke identificatiecode (gebruikers-ID) bedoeld voor persoonlijk gebruik conform de Nederlandse Norm NEN7510 Informatiebeveiliging in de

Zorg, par.11.5.2.. Op deze manier kunnen gebruikers worden gekoppeld aan en verantwoordelijk gesteld worden voor hun handelingen. Het verlenen van een groepsidentificatie wordt uitsluitend overwogen als dat noodzakelijk is vanwege bedrijfs- of operationele overwegingen en vraagt een formele goedkeuring (NEN7510 par. 11.2.1).

12. Het is niet toegestaan illegale en/of malafide software, bestanden of informatie op de werkplek te (laten) plaatsen c.q. installeren.
13. Het is de gebruiker niet toegestaan IT-middelen van het MUMC+ onbeheerd achter te laten waardoor onbevoegde toegang tot informatie en systemen mogelijk wordt.

Buiten gebruikstelling

14. Wanneer IT-middelen definitief niet meer gebruikt worden is de eigenaar c.q. (gedelegeerd) gebruiker verantwoordelijk voor het tijdig aanbieden van de apparatuur c.q. media aan MIT voor een gecoördineerde afvoer (ODIN 005414).
15. Om verantwoorde afvoer van datadragers te garanderen worden deze gedeponeerd in de daarvoor bestemde DigiBoxen (ODIN 0022423).

Artikel 4 Specifieke gebruiksregels

Lid:

1. De Raad van Bestuur kan toegang tot of gebruik van bepaalde vormen van IT verbieden; deze zijn opgenomen als bijlage B bij dit reglement.

Omgang met ICT-middelen

2. Bij handelen met (onderdelen van) de IT-middelen van MUMC+ geldt:
   i. de gebruiker die een vermoeden heeft dat zijn handelen binnen de informatievoorziening van MUMC+ tot schade leidt of zou kunnen leiden, is verplicht dit direct te melden aan zijn leidinggevende;
   ii. het gebruik van de internet voorziening is alleen toegestaan voor zakelijke en professionele doeleinden.
   iii. gebruik van (onderdelen van) de IT-middelen met een persoons-eigen commercieel oogmerk is niet toegestaan;
   iv. de gebruiker zal zich nimmer voordoen als een andere gebruiker dan wel gebruik maken van de bevoegdheden van een andere gebruiker;
   v. de gebruiker respecteert te allen tijde het intellectuele eigendom met betrekking tot onder meer auteurs, databanken, octrooien, merken, handelsnamen, tekeningen, modellen en de naburige rechten;
   vi. de gebruiker meldt alle incidenten bij de MIT Klantenservice. Tot incidenten worden zeker gerekend: inbreuken op de informatiebeveiliging (virus-, malware- en phishingmeldingen) fouten in applicaties en overtredingen van dit reglement en andere relevante reglementen, regelingen en wetten. De gebruiker meldt incidenten die leiden tot gevaarlijke situaties voor patiënt- en medewerkers in IRIS.
   vii. De gebruiker meldt incidenten met betrekking tot onbevoegde toegang tot ruimtes bij de meldkamer beveiliging.

Omgang met informatie

3. In Nederland is o.a. in de Wet Bescherming Persoonsgegevens vastgelegd dat en hoe de vertrouwelijkheid van persoonsgegevens door de verwerkende instanties (het MUMC+) dient te worden gegarandeerd. Deze wetgeving is door het MUMC+ voor intern medewerker gebruik vertaald in interne regelgeving. Onbevoegde toegang tot persoonsgegevens is op basis van de wet strafbaar.
4. Ten aanzien van vertrouwelijkheid van bedrijfsgegevens heeft de Raad van Bestuur eigen aanvullende regelgeving vastgesteld en gepubliceerd. Bij inbreuk op deze vertrouwelijkheid kan de Raad van Bestuur sancties opleggen aan individuele medewerkers.
5. Binnen het MUMC+ zijn er specifieke beleids- en gebruiksrichtlijnen voor het al of niet verstrekken van patiënt-, medewerker-, student- en bedrijfsgegevens. Deze zijn vastgelegd in het *Beleidsstandpunt verstrekking vertrouwelijke gegevens* (ODIN 004524) en het *Handboek bij toepassing beleid verstrekking vertrouwelijke gegevens* (ODIN 029592). Binnen dit aan-

dachtsgebied speelt privacy van patiënten, medewerkers en studenten een belangrijke rol. Het MUMC+ kent een privacy reglement dat verwijst naar de diverse regels en aandachtspunten hierin (ODIN 000532).

6. Distributie of beschikbaar stellen patiënt gerelateerde informatie via standaard internet of externe e-mail is niet toegestaan (bv. Dropbox, ftp). Voor alle gebruikers van deze faciliteiten geldt verder een gedragscode als gespecificeerd in document *Gedragscode voor het gebruik van internet en e-mail voor azM medewerkers* (ODIN 022408). Intern binnen het azM netwerk is dit vanuit beveiligingsoogpunt toegestaan. Blijft onverlet dat de verzender zich er van dient te vergewissen dat de geadresseerden recht hebbend is.
7. Voor de gebruiker geldt dat hij/zij slechts dan vertrouwelijke gegevens (met inbegrip van persoonsgegevens) per e-mail of internet verstuurt wanneer er aan de vereiste beveiliging en vertrouwelijkheid is voldaan. Dit betekent o.a. dat de inhoud uitsluitend door die geadresseerde(n) kan worden gelezen, die ook een recht hebben op toegang tot de gegevens.
8. Bij het constateren van een (vermeende) datalek situatie dient hiervan direct melding te worden gemaakt in IRIS.

Handelen in publiek domein

9. Bij handelen in het publieke domein (bv. internet, blogs, e-mail, *social media*) geldt bovendien het volgende:
   i. de gebruiker onthoudt zich van handelingen die tot schending van wettelijke bepalingen leiden;
   ii. de gebruiker vermijdt zoveel mogelijk de kans dat kwaadaardige code wordt binnengehaald of op andere wijze (onderdelen van) de IT-middelen van het MUMC+ met kwaadaardige code worden besmet. Mocht dit toch gebeuren dan dient dit per direct gemeld te worden bij de MIT klantenservice zodat adequate maatregelen genomen kunnen worden;
   iii. de gebruiker die ten onrechte gevoelige gegevens (waaronder persoonsgegevens) ontvangt dient de afzender onverwijld van dit feit op de hoogte te brengen;
   iv. de gebruiker zal zich slechts op gepaste en prudente wijze in het publieke domein gedragen, geen gevoelige gegevens (waaronder persoonsgegevens) openbaren aan anderen, de wet daarbij in acht nemen en de reputatie van MUMC+ niet schenden (zie artikel 4 lid 3);
   v. ter ondersteuning van het verantwoord internet gebruik (surfen e.a.) zijn er bestuurlijke en technische maatregelen getroffen (ODIN 003488).
   vi. Het MUMC+ heeft richtlijnen voor gedragingen van medewerkers op *social media* vastgelegd. Deze zijn te vinden op ODIN (ODIN procedures *Social Media, omgaan met Twitter, Hyves, Linkedin* nummer 004486).

Artikel 5 Toezicht

Lid:

1. Het MUMC+ (MIT) monitort continu de werking van de verschillende onderdelen van de informatievoorziening van het MUMC+ op adequate werking ten behoeve van de bewaking op ongewenste effecten op de betrouwbaarheid, integriteit en de vertrouwelijkheid. Voor zover mogelijk wordt daarbij de identiteit van gebruikers niet geopenbaard en de vertrouwelijkheid van gegevens en werkzaamheden niet geschonden. Voorbeelden van niet gewenste effecten zijn onbevoegde toegang tot en onbevoegde uitstroom van gegevens.
2. Wanneer beheerders van informatievoorzieningen (bv. een functioneel of technisch beheerder) gedragingen van gebruikers ontdekken die op welke wijze ook (mogelijk) een bedreiging vormen voor de informatievoorziening van MUMC+, dan mogen zij in alle redelijkheid en billijkheid in de voorzieningen corrigerend en indien nodig beperkend optreden op aspecten als bijvoorbeeld beschikbaarheid van en de toegang tot de voorzieningen en brengen daarvan de gebruiker en zijn/haar leidinggevende als ook de betreffende MIT manager onverwijld op de hoogte. Indien van toepassing vindt optreden naar een medewerker plaats op basis van onder andere artikel 5, 6 en 7 van dit reglement.
3. Specifiek voor internet geldt (volledige gedragscode zie ODIN 022408):
   i. Het gebruik van internet wordt vastgelegd met een maximale terugkijk interval van 1 maand.

ii. Op het gebruik van internet kan worden toegezien door steekproefsgewijze controle en aan de hand van geanonimiseerde lijsten van de bezochte internet sites.
iii. In het geval van een ernstig vermoeden van gebruik van internet of e-mail in strijd met deze gedragscode wordt het gebruik van de medewerker gecontroleerd aan de hand van de registratie van diens gebruik. Deze controle kan slechts en alleen plaatsvinden na schriftelijke melding aan en met schriftelijke goedkeuring van de Raad van Bestuur (zie ook artikel 6 lid 1).
iv. De aldus verkregen gegevens worden bewaard zolang dat voor het onderzoek en de afwikkeling daarvan noodzakelijk is.

4. Melding:
   i. Bij gedragingen door een gebruiker zoals bedoeld in het tweede lid kan een beheerder melding doen aan de gemandateerde leidinggevende van de betreffende gebruiker.
   ii. Of een melding wordt gedaan hangt af van de ernst van de gedraging, eventuele recidive en de wijze waarop de gebruiker reageert naar aanleiding van de constatering van de gedraging.
   iii. In het geval dat de gebruiker een vertrouwensfunctie vervuld, wordt de melding gedaan aan Functionaris Gegevensbescherming.
   iv. De Raad van Bestuur stelt vast wie in het kader van reglement wordt aangemerkt als vervuller van een vertrouwensfunctie.
5. De beheerders leggen vast in een toezichtslog:
   i. de wijze waarop, de tijdvakken waarbinnen monitoring plaatsvindt, alsmede de betrokken objecten van monitoring;
   ii. ontdekte bedreigende gedragingen, daarop genomen corrigerende acties en communicatie met betrokken gebruiker en leidinggevenden van beide partijen.
6. Toezichtslog:
   i. Het beheer van het toezichtlog berust bij Stafdirecteur MIT.
   ii. Het toezichtslog is slechts toegankelijk voor beheerders, Functionaris Gegevensbescherming en andere (in- en externe) toezichthouders.
   iii. Het toezichtslog mag slechts worden aangevuld en niet worden gewijzigd.
   iv. Gegevens in het toezichtslog moeten ten minste vier jaar doch mogen niet langer dan vijf jaar worden bewaard.

Artikel 6 Overtredingen

Lid:

1. Onderzoek:
   i. Bij een reëel vermoeden dat een gebruiker dit reglement en/of andere relevante reglementen, regelingen en wetten overtreedt, kan de gemandateerde leidinggevende van de gebruiker hiernaar onderzoek laten verrichten. Een verzoek hiertoe wordt ingediend bij de Raad van Bestuur.
   ii. De Raad van Bestuur geeft toestemming óf en hoe er daadwerkelijk onderzoek mag worden verricht.
   iii. In dit onderzoek worden de individuele gegevens omtrent het gedrag en de gedragingen van de betrokken gebruiker betrokken.
   iv. Door tussenkomst van Functionaris Gegevensbescherming kan het toezichtslog hier eveneens in worden betrokken.
   v. De Raad van Bestuur verstrekt de onderzoeksopdracht rechtstreeks aan de Manager informatiebeveiliging, de gemandateerd leidinggevende wordt geïnformeerd. Het onderzoek zal door één of meer leden van het MUMC-CSIRT worden uitgevoerd.
2. De gemandateerde leidinggevende stelt tegelijkertijd de gebruiker op de hoogte over de aard en de inhoud van het vermoeden en de inhoud van de onderzoeksopdracht, tenzij dit het onderzoek kan schaden. De onderzoeker i.s.m. de Manager Informatiebeveiliging rapporteert naar aanleiding van diens onderzoek aan de Raad van Bestuur en de gemandateerde leidinggevende.
3. De gemandateerde leidinggevende verstrekt onverwijld een afschrift van deze rapportage aan de gebruiker en stelt hem in de gelegenheid om zijn standpunt ter zake kenbaar te maken.

4. Nadat de gebruiker de kans heeft gehad zijn standpunt kenbaar te maken, stuurt de gemandateerd leidinggevende van het onderzoek een geanonimiseerde kopie van zowel het onderzoeksrapport als de reactie van de betrokkene daarop ter informatie aan de Functionaris Gegevensbescherming.

Artikel 7 Maatregelen en sancties

Lid:

1. Hangende een vermoeden of afgaande op een onderzoeksrapport kan de gemandateerde leidinggevende voorafgaande aan zijn definitieve besluit en met inachtneming van hetgeen daarover in de collectieve arbeidsovereenkomst is bepaald, een gebruiker met onmiddellijke ingang diens toegang tot (onderdelen van) de (geautomatiseerde) informatievoorziening beperken of intrekken.
2. De gemandateerde leidinggevende kan na constatering dat betrokkene dit reglement en/of andere relevante reglementen, regelingen en wetten heeft overtreden (op basis van het onderzoeksrapport en de reactie daarop van de betrokkene) de directeur van Strategie Personeel en Organisatie verzoeken om een traject disciplinaire maatregel conform hoofdstuk 11 Cao UMC te starten. Verwezen wordt naar het ODIN document “disciplinaire maatregel bij plichtsverzuim (022341).
3. Een sanctie kan conform art 11.2 Cao Umc variëren van een schriftelijke berisping tot strafontslag en is afhankelijk van ernst, omstandigheden en voorgeschiedenis conform vigerend personeelsbeleid.
4. Een kopie van het volledige sanctiebesluit wordt verstrekt aan de Corporate Security Officer.
5. De gemandateerde leidinggevende doet op advies van de Corporate Security Officer aangifte bij opsporingsinstanties en/of toezichthouders.

Artikel 8 Slotbepalingen

Lid:

1. De gemandateerde leidinggevende draagt er zorg voor dat alle onder hem ressorterende gebruikers op de hoogte zijn van dit reglement.
2. Voor al het in dit reglement gestelde kan de Raad van Bestuur nadere regels stellen. De volledige en actuele set richtlijnen is opgenomen in ODIN.
3. Dit reglement is door de Raad van Bestuur van MUMC+ vastgesteld op 17 maart 2016 en treedt met ingang van 1 mei 2016 in werking.
4. Drie jaar na inwerkingtreding wordt dit reglement in samenwerking met onder meer de Ondernemingsraad geëvalueerd.

Bijlage A Richtlijnen voor veilige omgang met gegevens

Lid:

1. Krachtens artikel 3 lid 5 kan de Raad van Bestuur nadere regels stellen aan de veilige omgang met gegevens. Deze regels luiden:
    i. De gebruiker maakt uitsluitend gebruik van centraal beheerde IT-faciliteiten van MUMC+ voor het veilig opslaan, verzenden en vernietigen van gegevens.

Bijlage B Verboden aspecten van IT

Lid:

1. Krachtens artikel 4 lid 1 kan de Raad van Bestuur bepaalde aspecten van IT verbieden. Verboden zijn:
    i. Opslag van gegevens van MUMC+ ‘in the cloud’ (zoals met behulp van dropbox, google-docs, wetransfer, Microsoft-live, Office-365).
    ii. Internet-telefonie (bijvoorbeeld skype).
    iii. Automatisch doorsturen (automatic forwarding) van e-mails met vertrouwelijke gegevens naar een e-mail-account buiten het mumc.nl-domein.
    iv. Peer-to-peer bestandsuitwisseling (zoals torrent en emule).
    v. Downloaden en/of gebruiken van zogenaamde hack-tools.
    vi. Downloaden en/of gebruiken van programma’s die louter privédoeleinden kennen.

vii. Bezoeken dan wel bestanden downloaden van sites waardoor de integriteit van het MUMC+ in het gedrang kan komen dan wel diens reputatie kan worden geschaad.

Implementatie van de doelstellingen

De verantwoordelijkheden voor de opzet van dit Reglement zijn beschreven in het document *Organisatie Informatiebeveiliging en Privacybescherming*. Ook de verantwoordelijkheden ten aanzien van het uitdragen en bewaken op de naleving zijn in dit document weergegeven. Een belangrijke taak is hierin weggelegd voor de managers van de medewerkers als ook voor de medewerkers onderling.

Verklaring van uitgifte

Geldigheid

Dit document in elektronische vorm is de enige geldige versie.

Fouten

Mocht u een fout ontdekken of een opmerking willen plaatsen gebruik hiervoor dan bij voorkeur de optie “opmerking plaatsen” in het betreffende document. U kunt ook contact opnemen met Documentmanagement via e-mail: ODIN @mumc.nl of via tst. 75990 of 71650.

Personalia

Documentcoördinator: J. Lamers, Stafadviseur Informatieveiligheid, Kwaliteit & Veiligheid, Patiënt & Zorg

Auteur(s): J. Lamers.

Beoordelaar(s): C. Aussems, Beleidsadviseur, Information Security Offic; J. Hanhart , Functionaris Gegevensbescherming; IT Steering Committee; R. Maenen, MIT Manager Unit Infrastructuur, Unit Klantenservice a.i., Unit Ontwikkeling a.i.; G. Martens, MIT Manager Informatiebeveiliging; R. Rademacher, MIT Manager Zorg, Unit SAP a.i., Unit Ondersteuning a.i.; B. Smeets, MIT Manager Kwaliteit en processen; I. Speetjens, Jurist

Inhoudelijk hoofdverantwoordelijke: J. Fiolet, Corporate Security Officer, Directeur-bestuurder Patiënt & Zorg

Autorisator: J. Fiolet, Corporate Security Officer, Directeur-bestuurder Patiënt & Zorg