Projectcode	-
Versie	Definitief
Datum	Versie 28 januari 2019
Opsteller	HR
Eigenaar	-
Opdrachtgever	Raad van Bestuur Erasmus MC

Gedragscode voor het gebruik van Internet en ICT-faciliteiten van het Erasmus MC

Inleiding

Veel Erasmus MC-medewerkers maken gebruik van Internet en ICT-faciliteiten. Het is van belang dat zorgvuldigheid wordt betracht bij dit gebruik. Aan het gebruik van Internet en ICT-faciliteiten, waaronder internet, e-mail en mobiele apparatuur, zijn grote voordelen, maar ook risico's verbonden. Daarom worden in deze gedragscode regels en voorwaarden gesteld waaraan aan het gebruik van Internet en ICT faciliteiten dient te voldoen. Bij het opstellen en toepassen van deze gedragscode is gestreefd naar een goede balans tussen controle op verantwoord gebruik van de computerfaciliteiten en de bescherming van de privacy van de werknemers. Schending van deze gedragscode kan leiden tot plichtsverzuim conform artikel 11.1 cao.

Bedacht moet worden dat ook derden werkzaamheden verrichten voor het Erasmus MC en daarbij gebruik maken van Internet en ICT-faciliteiten van het Erasmus MC. De gedragscode wordt op deze derden van toepassing verklaard middels de overeenkomst die met deze derden wordt gesloten.

In algemene zin, mocht het gebruik van Internet en ICT-faciliteiten dan wel de controle daarop gepaard gaan met het verwerken van persoonsgegevens, dan dient deze verwerking te voldoen aan de vereisten van de AVG. De verwerking wordt in ieder geval opgenomen in het Verwerkingenregister van de organisatie. Als vervolgens vastgesteld wordt, dat aan een dergelijke verwerking (privacy)risico’s verbonden zijn, dan kan het zijn dat een privacy impact assessment – volgens de AVG – moet worden uitgevoerd.

Erasmus MC zal geen oneigenlijk gebruik maken van de mogelijkheden om het gebruik van internet en ICT-faciliteiten door medewerkers te controleren.

Doelstellingen

Het instellen van deze gedragscode heeft tot doel de regels en voorwaarden voor het gebruik van Internet en ICT-faciliteiten, inclusief de wederzijdse rechten en plichten van de werkgever en de werknemer, bekend te maken. Daarnaast wordt beoogd de volgende risico’s te beperken en te voorkomen dat:

- Misbruik en overbelasting van de Internet en ICT-faciliteiten ontstaat.
- Incidenten of schade door het gebruik van de Internet en ICT-faciliteiten optreedt.
- Vertrouwelijke informatie van patiënten, werknemers, studenten of in het algemeen van het Erasmus MC ongeoorloofd wordt ontsloten aan derden.

Begripsbepalingen

Medewerker:	degene die een dienstverband heeft met het Erasmus MC dan wel anderszins onder de verantwoordelijkheid van het Erasmus MC is aangesteld.

Persoonsgegeven:	alle informatie over een geïdentificeerde of identificeerbare persoon “de betrokkene”. Als identificeerbaar wordt beschouwd een natuurlijk persoon die direct of indirect kan worden geïdentificeerd, met name aan de hand van een identificator zoals een naam, een identificatienummer, locatiegegevens, een online identificator of van een of meer elementen die kenmerkend zijn voor de fysieke, fysiologische, genetische, psychische, economische, culturele of sociale identiteit van die natuurlijke persoon.
Geautomatiseerde informatiesystemen:	gegevensverwerkende systemen met als activiteiten het verzamelen, verwerken, bewerken, bewaren, overdragen en verstrekken van gegevens die worden gebruikt bij de bedrijfsprocessen van het Erasmus MC waarbij gebruik wordt gemaakt van Internet en ICT-faciliteiten.
Vertrouwelijke informatie:	informatie waarvan de medewerker weet of dient te begrijpen dat het informatie betreft die niet ongeautoriseerd aan anderen bekend mag worden gemaakt. Hieronder wordt in ieder geval begrepen persoonsgegevens, zoals gedefinieerd in de Algemene Verordening Gegevensbescherming, waaronder patiëntgegevens en medewerkersgegevens, onderzoeksgegevens en concurrentiegevoelige gegevens.
Beheerder:	medewerkers van de pijler I&T van het Servicebedrijf die belast zijn met toezicht en beheer op het functioneren van de Internet en ICT-faciliteiten van het Erasmus MC. Dit betreft onder andere medewerkers van de **ICT-**Servicedesk, beheer van werkplekken, servers, netwerk, maken van back-up.
CERT:	Computer Emergency Response Team.
Internet en ICT-faciliteiten:	alle ICT-hulpmiddelen die worden gebruikt voor de uitvoering van de bedrijfsprocessen van het Erasmus MC, waaronder: (mobiele) apparatuur in eigendom of in bruikleen van Erasmus MC, programmatuur, netwerken en (mobiele) apparatuur in eigendom van de medewerker in gebruik voor werkdoeleinden.
Mobiele apparatuur:	laptop, tablet, smartphone, digitale gegevensdragers en eventuele andere draagbare Internet en ICT-faciliteiten.

Spam:	ongewenste berichten die via e-mail en sociale media verspreid worden.
Sociale media:	online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Voorbeelden van platformen zijn weblogs, video- en fotosites, microblogs en sociaal netwerksites. De bekendste voorbeelden hiervan zijn respectievelijk YouTube, Pinterest, Twitter en Facebook.

1. Werkingssfeer

Deze gedragscode is van toepassing op de medewerker die zich via Internet en ICT-faciliteiten toegang verschaft tot geautomatiseerde informatiesystemen die door of namens het Erasmus MC worden aangeboden.

De Gedragscode is eveneens van toepassing indien deze in een overeenkomst met een derde van toepassing is verklaard en deze derde zich via Internet en ICT-faciliteiten toegang verschaft tot geautoriseerde informatiesystemen die door of namens het Erasmus MC worden aangeboden. In dat laatste geval moet waar in deze Gedragscode ‘medewerker’ staat, ‘derde’ worden gelezen.

2. Gebruik algemeen

2.1 De aan de medewerker ter beschikking gestelde Internet en ICT-faciliteiten zijn bedoeld voor gebruik in het kader van de taak/functie-uitoefening. Privégebruik is alleen toegestaan voor zover dit de dagelijkse werkzaamheden niet negatief beïnvloedt en niet schadelijk is voor de (prestaties van) Internet en ICT-faciliteiten van het Erasmus MC.

2.2. Het is niet toegestaan Internet en ICT-faciliteiten van het Erasmus MC te gebruiken of te exploiteren voor commerciële doeleinden anders dan die welke voortvloeien uit hoofde van de taak/functievervulling.

2.3 Het is niet toegestaan informatie die strijdig is met de wet of de goede zeden (o.a. pornografisch materiaal), informatie die de goede naam van het Erasmus MC aantast, informatie die een discriminerend, opruiend, aanstootgevend of bedreigend karakter heeft met behulp van Internet en ICT-faciliteiten van het Erasmus MC te produceren, benaderen, op te slaan, te verspreiden of in de openbaarheid te brengen, tenzij dit uit oogpunt van medische behandeling en/of wetenschappelijk onderzoek noodzakelijk is.

2.4 De door het Erasmus MC ter beschikking gestelde programmatuur, hardware, gegevensbestanden of documentatie mogen niet ongeautoriseerd worden gekopieerd of ter beschikking worden gesteld aan derden.

2.5 De medewerker zal geen acties ondernemen of pogingen hiertoe doen die de continuïteit of de beveiliging van de Internet en ICT-faciliteiten van het Erasmus MC ondermijnen.

2.6 Bij afwezigheid van de medewerker draagt hij er zorg voor dat zijn computer/mobiele apparatuur is afgesloten of beveiligd is door middel van een screensaver met

wachtwoord, conform het 'clear desk' en 'clear screen' beleid Erasmus MC. Beiden zijn te vinden op Intranet.

2.7 Bij gebruik van digitale gegevensdragers (zoals USB-sticks) dient opslag van vertrouwelijke informatie versleuteld plaats te vinden. De medewerker vindt instructies hiervoor op de Service Portal van het Erasmus MC.

2.8 Bij het printen van vertrouwelijke informatie dient de medewerker ervoor zorg te dragen dat deze gegevens niet bij anderen terecht kunnen komen.

3. Toegang tot de Internet en ICT-faciliteiten

3.1 Toegang tot Internet en ICT-faciliteiten van het Erasmus MC wordt verleend op basis van een combinatie van gebruikersnaam (microsectienummer) en een persoonlijk wachtwoord of andere vergelijkbare identificatie- en authenticatiemiddelen (zoals smartcards en tokens). Deze zijn persoonlijk en niet overdraagbaar.

3.2 De medewerker draagt er zorg voor dat:
- het wachtwoord niet aan anderen bekend wordt;
- de persoonlijk toegekende identificatie- en authenticatiemiddelen niet gebruikt worden door anderen;
- bij constatering van misbruik van zijn combinatie van gebruikersnaam en wachtwoord of overige identificatie- en authenticatiemiddelen de ICT-Servicedesk hiervan onverwijld in kennis wordt gesteld en het wachtwoord direct gewijzigd wordt.

3.3 De medewerker wordt periodiek verzocht (via het systeem) om zijn wachtwoord te wijzigen.

3.4 Ten aanzien van afdelingsaccounts dan wel accounts die gedeeld worden met meerdere personen, wordt het daaraan gekoppelde wachtwoord gedeeld met de personen die hiertoe toegang dienen te hebben. Ten aanzien van derden die geen toegang dienen te hebben tot het gedeelde account is artikel 3.2 van overeenkomstige toepassing. De verantwoordelijke voor het gedeelde account regelt de toegang en ontzegging van toegang tot het gedeelde account, inclusief wijziging van het wachtwoord in geval de groep toegangsgerechtigden verandert en maakt bij gebruikers bekend met wie het wachtwoord mag worden gedeeld en maakt, indien van toepassing, afspraken met de gebruikers van het gedeelde account voor de waarborging van de bescherming van persoonsgegevens.

4. Regels en voorwaarden voor het gebruik van e-mail en internet

4.1 Het gebruik van het aan de medewerker op persoonlijke titel ter beschikking gestelde e-mailadres is strikt persoonlijk. Niet persoonsgebonden e-mailadressen kunnen wel met meerdere medewerkers worden gedeeld, waarbij altijd één medewerker als aanspreekpunt voor het e-mailadres wordt aangewezen. Artikel 3.2 is van overeenkomstige toepassing.

4.2 Het is de medewerker niet toegestaan om:
a) Een niet voor hem geldend e-mailadres te gebruiken tenzij de medewerker hiertoe door de rechtmatige gebruiker van het e-mailadres via zijn e-mailaccount gemachtigd is.
b) Met behulp van de Internet en ICT-faciliteiten van het Erasmus MC spam te versturen.

c) Met behulp van de Internet en ICT-faciliteiten anderen te pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins te beschadigen.
d) Voor andere medewerkers bestemde e-mailberichten doelbewust ongeautoriseerd te lezen, kopiëren, wijzigen, door te sturen of te vernietigen. Ontvangt de medewerker onbedoeld een mailbericht bedoeld voor een ander, dan stuurt hij deze door naar de juiste persoon en/of informeert hij de verzender en verwijdert de mail uit zijn mailbox.
e) Informatie te verzenden die strijdig is met de wet of de goede zeden (o.a. pornografisch materiaal), de goede naam van het Erasmus MC aantast en/of een discriminerend, opruiend, aanstootgevend of bedreigend karakter heeft tenzij dit uit oogpunt van medische behandeling en/of wetenschappelijk onderzoek noodzakelijk is.
f) Persoonsgegevens, waaronder patiëntgegevens en medewerkersgegevens, onbeveiligd te verzenden naar een niet Erasmus MC e-mailadres dan wel naar een Erasmus MC e-mailadres waarvan de gerechtigde niet geautoriseerd is om van de gegevens kennis te nemen, en in zijn algemeenheid vertrouwelijke informatie zonder gerechtvaardigd doel en/of rechtsgrond via internet onbeveiligd ter beschikking te stellen en/of onbeveiligd via openbare netwerken te verspreiden.
g) Elektronische kettingbrieven of waarschuwingsberichten van virussen aan (groepen van) medewerkers te verzenden.
h) Auteursrechtelijk beschermd materiaal, waaronder programmatuur, teksten, beeldmateriaal of muziek, te kopiëren, te downloaden via de faciliteiten van het Erasmus MC, of materiaal van Erasmus MC of derden ter beschikking te stellen zonder toestemming van de rechthebbende.

4.3 De medewerker dient bij downloaden van materiaal alles in het werk te stellen om het binnenhalen van bijv. virussen te voorkomen en de beschikbaarheid van de Internet en ICT-faciliteiten voor anderen niet in gevaar te brengen.

4.4 Het is toegestaan vertrouwelijke informatie over het interne netwerk te versturen (van en naar een Erasmus MC e-mailadres (@erasmusmc.nl)) voor zover verzender en ontvanger gerechtigd zijn tot deze informatie.

4.5 Een medewerker mag vertrouwelijke informatie die op het intranet van Erasmus MC is geplaatst niet kopiëren en op enigerlei wijze verspreiden .

5. Gebruik van sociale media

5.1 De gebruikers van sociale media dienen rekening te houden met de goede naam van het Erasmus MC en van een ieder die betrokken is bij het Erasmus MC. Privémeningen van medewerkers kunnen eenvoudig verward worden met de officiële standpunten van het Erasmus MC en het is aan de medewerker om dit te voorkomen. Artikel 2.1 is op het gebruik van sociale media onverkort van toepassing.

5.2 Het is toegestaan om kennis en informatie te delen, mits het geen vertrouwelijke of persoonsgegevens betreft waarvoor geen toestemming is gegeven deze te delen en andere betrokkenen of het Erasmus MC niet schaadt.

5.3 De medewerker is persoonlijk verantwoordelijk voor de inhoud welke hij publiceert op de sociale media.

5.4 Wees ervan bewust dat de gepubliceerde teksten en uitlatingen voor onbepaalde tijd openbaar zullen zijn, ook na verwijdering van het bericht.

5.5 Het is voor medewerkers niet toegestaan om foto-, film- en geluidsopnamen van aan het Erasmus MC gerelateerde situaties op sociale media te zetten, tenzij hiervoor door betrokkenen en door de afdeling Communicatie van het Erasmus MC uitdrukkelijk toestemming voor plaatsing is gegeven.

5.6 Medewerkers nemen algemeen geldende fatsoensnormen in acht. Als fatsoensnormen worden overschreden (bijvoorbeeld: pesten, kwetsen, stalken, bedreigen, zwartmaken of anderszins beschadigen) dan heeft het Erasmus MC het recht passende maatregelen te nemen.

6. Gebruik ter beschikking gestelde mobiele apparatuur

6.1 Aan de medewerker kan ter uitvoering van zijn werkzaamheden mobiele apparatuur ter beschikking worden gesteld. De medewerker dient hierbij een bruikleenovereenkomst te ondertekenen.

6.2 Bij diefstal of vermissing van de mobiele apparatuur, dient de medewerker per direct melding daarvan te doen bij de ICT Servicedesk en aangifte te doen bij de politie. In geval er sprake is van een datalek wordt een melding gedaan van dit datalek volgens de hiervoor binnen het Erasmus MC geldende procedure (zie Intranet).

6.3 Indien de medewerker zich met de mobiele apparatuur toegang tot e-mail en agenda wil verschaffen en/of toegang tot intranet via een ander netwerk dan het Erasmus MC-netwerk, dan is dat alleen mogelijk via het installeren van de door de Raad van Bestuur vastgestelde applicatie(s) (app(s)). Deze app(s) zijn bedoeld om vertrouwelijke informatie binnen de beschermde Erasmus MC-omgeving te houden. Voor installatie van de app(s) is toestemming van de leidinggevende noodzakelijk.

6.4 De medewerker mag geen vertrouwelijke gegevens opslaan op (de harde schijf van) mobiele apparatuur tenzij dit versleuteld plaatsvindt. De medewerker vindt instructies voor versleuteling op de Service Portal van het Erasmus MC.

7. Gebruik van mobiele apparatuur in eigendom van de medewerker

7.1 De medewerker kan voor de uitvoering van zijn werkzaamheden gebruik maken van zijn eigen mobiele apparatuur. De medewerker blijft verantwoordelijk voor zijn eigen apparatuur en dient zorg te dragen voor de noodzakelijke beveiliging, zoals toegangscode en versleuteling. Er wordt geen ondersteuning geboden voor onderhoud en beheer vanuit het Erasmus MC, behalve ten aanzien van de door het Erasmus MC ter beschikking gestelde en verplichte app(s).

7.2 Indien de medewerker zich met de eigen mobiele apparatuur toegang tot e-mail en agenda wil verschaffen en/of toegang tot intranet via een ander netwerk dan het Erasmus MC netwerk, dan is dat alleen mogelijk via het installeren van de door de Raad van Bestuur vastgestelde app(s). Deze app(s) zijn bedoeld om vertrouwelijke informatie binnen de beschermde Erasmus MC-omgeving te houden. Voor installatie van de app(s) is toestemming van de leidinggevende noodzakelijk.

7.3 Bij diefstal of vermissing van de eigen mobiele apparatuur waar de verplichte app(s)op zijn geïnstalleerd, dient de medewerker per direct melding daarvan te doen bij de ICT Servicedesk zodat de Erasmus MC app(s) en informatie op afstand kunnen worden verwijderd. Bij vermoeden van een datalek wordt een melding gedaan volgens de hiervoor binnen het Erasmus MC geldende procedure (zie Intranet).

7.4 De medewerker mag, buiten de app(s) als bedoeld in artikel 7.2, geen vertrouwelijke informatie opslaan op (de harde schijf) van de eigen mobiele apparatuur tenzij dit versleuteld plaatsvindt. De medewerker vindt instructies voor versleuteling op de Service Portal van het Erasmus MC.

8. Niet persoonsgerichte controle e-mail en internet

8.1 In het kader van systeem- en netwerkbeveiliging en ter voorkoming en detectie van overtreding van de gedragsregels zoals opgenomen in dit reglement kan het e-mail- en internetgebruik op geautomatiseerde wijze en niet-persoonsgericht worden gecontroleerd (inclusief privé e-mailberichten die via het Erasmus MC netwerk worden verstuurd), dit wordt 24 uur per dag grotendeels geautomatiseerd gedaan.

8.2 Het op geautomatiseerde wijze en niet-persoonsgerichte controleren betreft:

a. het controleren op schadelijke bestandsformats en virushandtekeningen;
b. het controleren op het automatisch doorzenden van e-mailberichten naar een e-mailadres dat niet door het Erasmus MC ter beschikking is gesteld;
c. het controleren op het downloaden van programmatuur;
d. het ten behoeve van kosten- en capaciteitsbeheersing analyseren van verkeersgegevens van e-mail en internetgebruik;
e. het door middel van content scanning controleren achteraf van e-mailberichten en internetverkeer op racistische en seksueel getinte inhoud of het ongeautoriseerd verspreiden van vertrouwelijke informatie.

8.3 De controle, bedoeld in het tweede lid, onderdeel e, is gericht op trefwoorden en grafische bestanden met bepaalde eigenschappen. Controle van het internetverkeer kan tevens plaats vinden aan de hand van namen van bezochte sites.

8.5 In het kader van technisch systeem- en netwerkbeheer vindt logging plaats. Hiermee kan worden vastgelegd welke data in een IT-systeem zijn verwerkt, verzameld, geraadpleegd, gewijzigd of gewist. Logbestanden zijn bedoeld om de integriteit en beveiliging van data te bevorderen. Ook kunnen zij waardevolle informatie verschaffen over bijvoorbeeld piekbelasting of over aanwezige softwarebugs. Deze gegevens worden niet langer dan een periode van zes maanden bewaard.[1]

9. Persoonsgerichte inhoudelijke controle

9.1 Indien de niet persoonsgerichte controle leidt tot een redelijk vermoeden of concrete feiten of omstandigheden dat een medewerker zich niet aan de gedragscode houdt en/of het belang van het Erasmus MC schendt, of er anders dan door een niet persoonsgerichte controle zoals bedoeld in het vorige artikel een redelijk vermoeden of concrete feiten of omstandigheden bestaan dat een medewerker zich niet aan de gedragscode houdt en/of het belang van het Erasmus MC schendt, kan in het kader van een onderzoek naar dit plichtsverzuim een gerichte controle uit worden gevoerd

[1] In de AVG zijn er geen (bewaar)termijnen opgenomen. De toets dat gegevens niet langer dan noodzakelijk mogen worden bewaard is gebonden aan het doel.
De AVG legt de verplichting op om alle datalekken rondom persoonsgegevens te documenteren. Om aan die documentatieplicht te voldoen moeten er adequate logbestanden zijn. De AP kan deze data namelijk ook opvragen. De bewaartermijn moet daarvoor wel lang genoeg zijn.

door het CERT en/of de eenheid Audit op e-mail-, netwerkverkeer of internetgebruik van individuele medewerkers. Van deze controle wordt een schriftelijke rapportage opgesteld.
Er geldt hierbij de volgende procedure:

- De Raad van Bestuur, de manager Audit dan wel de leidinggevende van de afdeling waar de medewerker die mogelijk schuldig is aan plichtsverzuim werkzaam is, verzoekt een onderzoek naar e-mail-, netwerkverkeer of internetgebruik van de medewerker. De arbeidsjurist wordt hiervan op de hoogte gesteld.
- Het CERT en/of de eenheid Audit legt de schriftelijke rapportage voor aan de Raad van Bestuur, de manager Audit dan wel de leidinggevende.
- Ten aanzien van mogelijke personele consequenties wordt de arbeidsjurist in een zo vroeg mogelijk stadium betrokken.
- De gegevens worden alleen gebruikt ten behoeve van het onderzoek naar het vermeende plichtsverzuim waarvoor de gegevens zijn opgevraagd en de eventuele besluitvorming die uit het onderzoek volgt.

9.3 Indien de schriftelijke rapportage zoals bedoeld in de voorgaande leden niet leidt tot verdere acties, dan wordt de rapportage binnen 1 maand vernietigd.

9.4 De medewerker wordt direct geïnformeerd over het feit dat er een onderzoek wordt ingesteld. Hiervan kan worden afgeweken indien dit in het belang van het onderzoek is. In dat geval wordt de voorzitter van de Ondernemingsraad in vertrouwen geïnformeerd.

9.5 Werknemers met een bijzondere vertrouwensfunctie zoals bedrijfsartsen, vertrouwenspersonen en de mediator, zijn in beginsel uit hoofde van hun functie die vertrouwelijkheid vereist uitgesloten van persoonsgerichte controle. Dit geldt niet voor de controle op de beveiliging van het berichtenverkeer.

9.6 Leden van de Ondernemingsraad of de Onderdeelcommissies zijn in beginsel in het kader van de uitoefening van hun werkzaamheden als lid van de Ondernemingsraad of Onderdeelcommissie uitgesloten van persoonsgerichte controle.
Dit geldt niet voor de controle op de beveiliging van het berichtenverkeer.

10. Beheer

10.1 Bij geconstateerde (beveiligings)incidenten heeft de beheerder het recht om medewerkers de toegang tot computers en/of netwerken (tijdelijk) te ontzeggen.

10.2 In afwijking van artikel 4.1 kan de mailbox van een medewerker met toestemming van deze medewerker worden overgedragen aan c.q. worden gedeeld met een andere medewerker. Indien de betreffende medewerker niet beschikbaar is en de voortgang van het werk dit vereist, kan door de beheerder aan de leidinggevende of een door de leidinggevende aangewezen vervanger toegang tot de mailbox van de medewerker verschaft worden.
Hiervan zal alleen sprake kunnen zijn indien de medewerker geen toestemming kan of wil geven en er geen andere manier is om de in de mail opgeslagen gegevens snel voor het werk beschikbaar te kunnen hebben. De medewerker wordt per direct geïnformeerd. De leidinggevende of vervanger mag zich geen toegang verschaffen tot mails die een privékarakter lijken te hebben, dan wel verzonden of afkomstig van een mediator, vertrouwenspersoon of bedrijfsarts.

10.3 Wanneer de beveiliging of de continuïteit van de mailvoorziening dit vereist, is de beheerder gerechtigd voor medewerkers bestemde berichten te kopiëren, verplaatsen, vernietigen of bijlagen te verwijderen. De medewerker wordt per direct hiervan in kennis gesteld.

10.4 Ten behoeve van het beheer van de Internet en ICT-faciliteiten wordt de op het netwerk aangesloten apparatuur en programmatuur regelmatig geïnventariseerd. De hieruit verzamelde gegevens worden door de beheerder vastgelegd en worden alleen ingezet voor het beheer van Internet en ICT-faciliteiten en niet voor andere doeleinden gebruikt.

11. Bijzondere bepalingen voor de beheerder

11.1 De beheerder is verplicht vertrouwelijke informatie en persoonsgegevens waar hij in het kader van de activiteiten als beheerder toegang toe heeft, strikt vertrouwelijk te behandelen. Schending van deze plicht kan worden gezien als plichtsverzuim. Op de naleving van dit artikel wordt toegezien door de eigen leidinggevende, door Audit en de CERT.

11.2 De beheerder dient activiteiten die inzage in vertrouwelijke informatie of persoonsgegevens van individuele werknemers vereisen, zo veel mogelijk te beperken.

11.3 De beheerders verschaffen zich slechts toegang tot accounts of Internet en ICT-faciliteiten van een werknemer als deze daarvoor zijn toestemming heeft gegeven. Toegang zonder deze toestemming is slechts toegestaan, in geval van een controle als bedoeld in artikel 9 of beheer als bedoeld in artikel 10 en vindt plaats op aanwijzing en onder toezicht van het CERT en/of Audit.

12. Overige bepalingen

12.1 Deze gedragscode kan met inachtneming van de ter zake geldende voorschriften en na instemming van de Ondernemingsraad, door de Raad van Bestuur worden aangevuld en gewijzigd.

12.2 In alle gevallen waarin deze gedragscode niet voorziet, beslist de Raad van Bestuur.

12.3 Wanneer aan deze gedragscode wordt gerefereerd wordt gesproken over “de Gedragscode Internet en ICT-faciliteiten”.

Aldus vastgesteld door de Raad van Bestuur op 10 december 2018.