DIJKLANDER ZIEKENHUIS

Titel	**Gedragscode: informatieveiligheid**
Locatie	**Purmerend én Hoorn**
Versie	5
Publicatiedatum	20-06-2024
Controledatum	20-06-2027

Wijzigingen ten opzichte van de vorige versie:
20/06/2024 Volledig herzien

		Beoordeeld op	Beoordelaar
Inhoudelijke beoordeling	14 dagen	20-06-2024 (Goedgekeurd)	Weelden, Eline van
Autorisatie	10 dagen	20-06-2024 (Goedgekeurd)	Bruijnincx, Jessica

ID nummer	15856
Map	Bestuursbureau
Specialisme	
Auteur	Revers-Bakker, Suzanne
Verzendlijst	

Titel	**Gedragscode: informatieveiligheid 0**
Locatie	**Purmerend én Hoorn**

Toepassingsgebied

Alle locaties van het Dijklander Ziekenhuis

Doel

Deze gedragscode maakt onderdeel uit van het Dijklander Ziekenhuis informatiebeveiligingsbeleid en beschrijft de gedragsregels voor individuele gebruikers van informatievoorzieningen en -systemen met betrekking tot patiëntengegevens en bedrijfsinformatie. Hieronder valt het zorgvuldig gebruik van ICT-middelen, zoals (mobiel) werkplekken, e-mail, internet, telefonie en informatie.

Doelgroep

Deze gedragscode is van toepassing op personeel in loondienst of niet in loondienst, die werkzaamheden voor het Dijklander Ziekenhuis verrichten en daarbij kan beschikken over internet-, e-mailfaciliteiten en/of telefoniesystemen en -voorzieningen.

Ziekenhuisbreed geldend

Ziekenhuisbreed geldend

Toelichting/ definities

Bij het opstellen van deze gedragscode is voorop gesteld dat de regels werkbaar moeten zijn en niet bedoeld zijn om de medewerkers in hun dagelijkse werkzaamheden te beperken. Het creëert een evenwicht tussen het praktisch beschikken over vertrouwelijke gegevens en beschermen van vertrouwelijke gegevens.

Het Dijklander Ziekenhuis beoogt met deze Gedragscode informatieveiligheid:

- Instructies te geven over wijze waarop gebruik moet worden gemaakt van informatiesystemen zoals de applicaties, waarin patiëntengegevens en bedrijfsinformatie worden verwerkt alsmede de internet-, e-mail- en telefoniefaciliteiten;
- Eventuele negatieve gevolgen van het gebruik van informatie en informatiesystemen zoals het risico op, computervirussen, het onbevoegd veranderen van informatie in patiëntendossiers of het schenden van de privacy van de patiënt voor het Dijklander Ziekenhuis te voorkomen en/of te beperken.

Uitgangspunten en toezicht

Eigen verantwoordelijkheid waar dat kan, regels en controle daar waar nodig, dat is het voornaamste uitgangspunt.

De medewerker is verantwoordelijk voor zijn gedrag rond zijn digitale voorzieningen. Daarbij werkt de medewerker met informatie die vaak vertrouwelijk is, betrouwbaar en beschikbaar moet zijn. Deze gedragscode geeft de medewerker handvatten. Het Dijklander Ziekenhuis verwacht van de medewerker dat die zich overeenkomstig de inhoud en de strekking van deze gedragscode gedraagt.

Gebruik maken van de geboden ICT-middelen betekent dat de medewerker instemt met logging van zijn/haar activiteiten op internet en in de e-mail. In specifieke situaties (b.v. bij vermoeden van een misdrijf) kan de logging worden ingekeken. Hiervoor is instemming nodig van de Functionaris Gegevensbescherming, als onafhankelijke toezichthouder op de AVG. Deze zal bij een dergelijk verzoek de privacy van de medewerker uitvoerig meewegen.

Definities

Informatiebeveiliging
Onder ‘informatiebeveiliging’ wordt verstaan: het stelsel van maatregelen voor het behoud van vertrouwelijkheid, integriteit en beschikbaarheid van gegevens, processen en informatiesystemen.

Informatiesysteem
Onder ‘informatiesysteem’ wordt verstaan: het geheel van mensen, middelen, procedures en regels dat de informatievoorziening verzorgt. Deze set van componenten heeft als doel informatie te verzamelen, verwerken, opslaan en verspreiden ter ondersteuning van de zorg, besluitvorming, coördinatie en controle binnen de organisatie.

Medewerker
Onder ’medewerker‘ wordt verstaan: personeel in loondienst of niet in loondienst, die werkzaamheden voor het Dijklander Ziekenhuis verrichten en daarbij kan beschikken over internet-, e-mailfaciliteiten en/of telefoniesystemen en -voorzieningen.

ICT-middelen

Het begrip ICT-middelen wordt hier breed opgevat, als alle hardware, software en diensten die tezamen een ‘digitale werkomgeving’ vormen.

- E-mailfaciliteiten: de door of namens het Dijklander Ziekenhuis aan Personeelsleden ter beschikking gestelde e-mailfaciliteiten waaronder een e-mailadres, mailbox en toegang van buiten het Dijklander Ziekenhuis;
- Internet- en andere netwerkfaciliteiten: de door of namens het Dijklander Ziekenhuis aan personeelsleden ter beschikking gestelde internet-toegang, waaronder ook via GSM 4/5G en Wi-Fi;
- Telefonie: de door of namens het Dijklander Ziekenhuis aan Personeelsleden ter beschikking gestelde telefoniefaciliteiten, waaronder bereikbaarheid (telefoonnummers en doorschakelfaciliteiten), voicemail en beltegoed.
- Werkplek: alle voor het uitoefenen van de functie noodzakelijke applicaties, toegang en gebruiksrechten en andere geïnstalleerde en online hulpmiddelen.
- ICT-apparatuur: alle huidige en toekomstige elektronische communicatie- en informatieapparatuur die door of namens het Dijklander Ziekenhuis aan Personeelsleden ter beschikking zijn of worden gesteld, zoals (mobiele) telefoon, tablet en laptop ter ondersteuning van de functie-uitoefening van de Personeelsleden.

Bijzondere gebruiksafspraken
Bij in gebruik nemen van ICT-middelen, netwerkaccount + wachtwoord gelden specifieke gebruiksafspraken die beschikbaar worden gesteld op het moment van verstrekking.

Inleiding

Deze Gedragscode is van toepassing op iedereen die gebruik maakt van de ICT-middelen van het Dijklander Ziekenhuis en is ook van toepassing op het werkgerelateerd online verkeer via privé ICT-middelen. Deze Gedragscode geldt voor alle personeelsleden. het Dijklander Ziekenhuis vraagt ook dat externen zich in lijn met deze Gedragscode gedragen en handelen. Ook als een persoon is ingehuurd, maar wel de beschikking krijgt over digitale faciliteiten is deze contractueel aan deze Gedragscode gebonden.

Medewerkers krijgen bij de aanvang of wijziging van een dienstverband en/of contract de beschikking over een vaste werkplek of een laptop en een ‘digitale werkomgeving’ (inlogaccount). Soms krijgt een medewerker ook een smartphone van het Dijklander Ziekenhuis. In sommige gevallen heeft de medewerker ook een tablet tot zijn beschikking.

Medewerkers krijgen van het Dijklander Ziekenhuis een volledige digitale werkomgeving aangeboden. Op mobiele middelen, zoals de smartphone en de tablet, worden beperkte functionaliteiten, zoals vergader-, agenda- en e-mailvoorzieningen verstrekt.

ICT-middelen bieden medewerkers mogelijkheden die een zeker risicobesef vragen. Daarom heeft het Dijklander Ziekenhuis in deze gedragscode de regels/afspraken omtrent het aanvaardbaar gebruik van ICT-middelen en veilig online samenwerken formeel vastgelegd.

Binnen het Dijklander Ziekenhuis geldt dat alle bedrijfsmiddelen eigendom blijven van het Dijklander Ziekenhuis en bij het beëindigen van een dienstverband en/of contract moeten worden ingeleverd. Binnen het Dijklander Ziekenhuis geldt:

- Alle uitgegeven bedrijfsmiddelen worden vastgelegd.
- Teruggave maakt onderdeel uit van off-boarding proces.
- Teruggegeven bedrijfsmiddelen worden gecontroleerd en schoongemaakt (verwijderen van alle informatie/gegevens/instellingen/etc.).
- Teruggegeven bedrijfsmiddelen worden vastgelegd.

Het is van belang dat de medewerkers bewust zijn van de risico’s rond het beheer van bedrijfsmiddelen. Dat stelt de medewerker in staat om zijn eigen verantwoordelijkheid te nemen. Daarom heeft het Dijklander Ziekenhuis naast de technische beveiliging voor het vergroten van de weerbaarheid deze gedragscode voor ICT-middelen opgesteld. Iedereen behoort zicht hieraan te houden en is hierop aanspreekbaar.

Benodigdheden

Regels voor het zorgvuldig gebruik van voorzieningen

Deze gedragscode beschrijft zo concreet mogelijk welk gedrag bij het gebruik van de ICT-middelen en informatie wordt verwacht.

Algemeen

De medewerker dient zich te houden aan de wet- en regelgeving met betrekking tot informatiebeveiliging, zoals (niet-limitatief) de regels die zijn vastgelegd in bijvoorbeeld de Algemene verordening gegevensbescherming (AVG), Wet meldplicht datalekken, de Wet geneeskundige behandelingsovereenkomst (WGBO) en de normeisen van NEN 7510.

Met het naleven van deze Gedragscode dragen medewerkers bij aan de betrouwbaarheid en weerbaarheid van de informatievoorziening van het Dijklander Ziekenhuis.

het Dijklander Ziekenhuis waarborgt met back-up en technische beveiligingsmaatregelen de beschikbaarheid, duurzame toegankelijkheid, integriteit en vertrouwelijkheid van de informatie. Niet alle risico's zijn echter technisch te ondervangen, waardoor afspraken over gebruik van digitale werkomgevingen en online gedrag nodig zijn. Veilig, effectief en efficiënt gebruik van ICT-middelen draagt bij aan de betrouwbaarheid en weerbaarheid van de informatievoorziening van het Dijklander Ziekenhuis.

Bij vermissing of het vermoeden van diefstal van (onderdelen van) digitale apparatuur en gegevensdragers dient de medewerker hiervan melding te maken bij de helpdesk ICT. Dit geldt dus niet alleen voor het melden van Dijklander Ziekenhuis middelen, maar ook privé apparatuur op of via zakelijke ICT-middelen.
Mobiele apparatuur en gegevensdragers (laptop, smartphone, usb-stick) mogen nooit ergens achter gelaten worden, zonder dat de medewerker heeft vastgesteld dat het voor onbevoegden onmogelijk is om toegang tot de informatie te krijgen.

De medewerker is verantwoordelijk voor de handelingen die worden verricht onder zijn persoonlijke toegang (inloggegevens) tot ICT-middelen en tot de apparatuur die hij voor zijn functie en werkzaamheden heeft ontvangen. Deze mogen niet aan anderen, ook niet aan de kinderen worden uitgeleend.

Elke medewerker kan op die verantwoordelijkheid worden aangesproken door de leidinggevende en door de functionaris gegevensbescherming. Inbreuk op deze gedragscode wordt beschouwd als plichtsverzuim. Dit kan verschillende sancties tot gevolg hebben, afhankelijk van de aard en ernst van het vastgestelde plichtsverzuim.

Schade, dat kan gebeuren

Schade kan onbedoeld ontstaan door het ontvangen en openen van verdachte bestanden. Een veel gebruikte manier om virussen of malafide software te verspreiden is (spear)phishing. Dat is een gerichte poging tot oplichting en het verkrijgen van inlog-, privé- en/of creditcard gegevens, door een schijnbaar persoonlijk bericht.

Wees alert op berichten waarin je onder druk wordt gezet of juist wordt verleid om gegevens te verstrekken of om op een link te klikken.

Vertrouw je het bericht niet, open de e-mail dan niet verder. Bel de helpdesk ICT en volg hun aanwijzingen op. Klik nooit op verdachte bijlagen, links, pop-ups en banners. Die bevatten vaak virussen en malafide software.

Schade kan ook ontstaan door software te installeren op de computers en laptops of door vanaf een mobiele gegevensdrager (usb-stick, externe harde schijf, etc.) software te draaien op deze digitale werkomgevingen. De ICT-beheerorganisatie heeft de mogelijkheid om dergelijke software te blokkeren.
Wanneer de betreffende functionaliteiten noodzakelijk zijn voor het werk, dan kan in overleg met én met toestemming van de leidinggevende een verzoek gedaan worden via de helpdesk ICT.

Het veranderen of omzeilen van de door de ICT-beheerorganisatie ingestelde beperkingen, of het hacken van ICT-middelen is niet toegestaan.

Internet

Van alle personeelsleden wordt professioneel en integer online handelen verwacht.
De informatiesystemen, e-mail faciliteiten en de internettoegang worden aan de medewerker voor zakelijk gebruik beschikbaar gesteld. Gebruik is dus onlosmakelijk verbonden met de taken die voortvloeien uit de functie.
Hoewel de toegang tot het internet bestemd is voor zakelijk gebruik is een kortstondig persoonlijk gebruik van het internet toegestaan mits dit niet storend is voor de dagelijkse werkzaamheden en het geen verboden gebruik oplevert.

Bij twijfel wordt de medewerker geacht overleg te plegen met de leidinggevende over het privé gebruik.

Het bezoeken van sites, downloaden of verzenden van informatie met een pornografische, racistische, discriminerende, extremistische, terroristische, aanstootgevende of – al dan niet seksueel - intimiderende of anderszins beledigende of bedreigende inhoud, is niet toegestaan. Zie hiervoor ook het Social media: Gedragscode / Omgaan met social media voor werknemers.

Verder is het niet toegestaan om via de internetfaciliteiten van het Dijklander Ziekenhuis:
- sites te bezoeken die bestemd zijn om te gokken en/of geld te verwerven dan wel het bezoeken van chat - en babbelboxen is niet toegestaan;
- materiaal te downloaden waarvan de gebruiker redelijkerwijs kan begrijpen dat het ziekenhuis zich daar niet mee kan verenigen of de goede naam van de zorginstelling schaadt;
- zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op internet;
- zich onbevoegd toegang te verschaffen tot systemen van andere organisaties;
- het e-mailadres en de naam van het ziekenhuis achter te laten op websites, tenzij dit werkgerelateerde websites zijn, zoals websites van beroepsorganisaties en/of –verenigingen;
- materiaal te downloaden en/of te installeren op de computer. Deze mogelijkheid is centraal zoveel mogelijk geblokkeerd. Indien het downloaden en/of installeren van materiaal voor de functie noodzakelijk is, dan is het verplicht dit te melden bij de supportdesk ICT en ten aanzien van de betrokken applicatie een risicoanalyse uit te voeren.
- software, gegevens of artikelen te downloaden of te kopiëren waarvoor licenties of auteursrechten gelden;

- bestanden vanuit het Dijklander Ziekenhuis te uploaden naar of beschikbaar te stellen aan derden buiten het netwerk van het ziekenhuis behalve in de situaties waarin daartoe een wettelijke verplichting bestaat.

Online samenwerken

De medewerker dient zich bij het delen van informatie telkens af te vragen of er schade kan ontstaan wanneer de informatie in handen komt van andere mensen dan voor wie de informatie bedoeld is (financiële-, imago-, juridische schade, et cetera).

De medewerker slaat vertrouwelijke of privacygevoelige gegevens nooit in gratis onlinediensten op.

Bij het gebruik van vertaalapps (zoals google translate of say hi) of chatbots voor taalverwerking (zoals Chat GPT) zorgt de medewerker ervoor dat hij/zij géén herleidbare persoonsgegevens opneemt in de app/bot. De medewerker zet er dus géén naam, geboortedatum, BSN, en dergelijke in.

E-mail

Het e-mailadres is bedoeld voor zakelijk gebruik.
Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- De medewerker is persoonlijk verantwoordelijk voor het gebruik van de aan hem of haar toegekende rechten voor systemen en middelen;
- Patiënt gerelateerde en/of bedrijfsgevoelige informatie mag niet per e-mail vanuit het Dijklander Ziekenhuis naar buiten worden verstuurd, tenzij het bericht op zodanige wijze is versleuteld dat de gegevens niet herleidbaar zijn;
- Bij patiënt gerelateerde informatie die direct tot de persoon herleidbaar is, dient de verzender zich ervan vergewist te hebben dat de ontvanger de privacy van de patiënt zal waarborgen;
- Patiëntengegevens mogen niet via een andere mailserver (zoals Hotmail, Gmail e.d.) dan die van het ziekenhuis verstuurd worden;
- Het is de medewerker niet toegestaan om aan derden (gedeelten van) het interne Dijklander Ziekenhuis adresboek met e-mailadressen beschikbaar te stellen.

Het is niet toegestaan om via de e-mailfaciliteiten van het Dijklander Ziekenhuis:
- Berichten anoniem of onder een fictieve naam te versturen.
- Ketting e-mailberichten te verzenden of door te sturen.
- Iemand lastig te vallen door middel van onnodige en/of ongewenste berichten.

Veilig e-mailen
Het veilig verzenden van e-mail berichten is gegarandeerd binnen het netwerk van het Dijklander Ziekenhuis, dus tussen medewerkers van het Dijklander Ziekenhuis hoeft geen extra beveiliging te worden gebruikt.

Bij het versturen van informatie naar externe e-mailadressen, zorgt de medewerker dat gevoelige gegevens beveiligd worden verstuurd. Medewerker volgt hierbij de regels zoals die zijn beschreven in Instructie Zivver: veilig mailen met ketenpartners en patiënten.

Zakelijke e-mail op privé telefoon/tablet

Dijklander ziekenhuis biedt alle medewerkers de mogelijkheid om hun zakelijke mail (op @dijklander.nl e-mailadres) te lezen op hun privé apparaat. Hierbij wordt de mail direct gesynchroniseerd tussen de mail omgeving (exchange) en een mobiel device (smartphone/tablet), waardoor je overal en continu de beschikking hebt over de laatste informatie. Bij het synchroniseren met het netwerk van het Dijklander Ziekenhuis gaat de medewerker akkoord met de onderstaande uitgangspunt van het Dijklander Ziekenhuis:

- Het ziekenhuis mag en kan de synchronisatie met een privé apparaat (smartphone/iPad) direct stopzetten.

Randvoorwaarden en verantwoordelijkheden voor gebruikers zijn:
- Medewerkers gaan zorgvuldig om met (vertrouwelijke) informatie. Zakelijke mail op privé telefoon/tablet is uitsluitend bedoeld voor zakelijk gebruik.
- Toegang tot de zakelijke mail gaat op basis van de uitgangspunten uit het beleid Gebruikerstoegang en authenticatie. De beveiliging van zakelijke mail mag niet worden uitgeschakeld of gewijzigd.
- Medewerkers dienen na het uitbrengen van (beveiligings)updates van de fabrikant deze zo spoedig mogelijk op het device te installeren.
- Medewerkers zijn alert op de beveiliging en veiligheid. Zij zijn gehouden aan het geldende beleid om incidenten en kwetsbaarheden met betrekking tot beveiliging en gebruik van informatie en communicatiemiddelen onmiddellijk te melden bij zijn/haar leidinggevende en als veiligheidsincident te melden bij de IT Servicedesk.
- Verlies en/of diefstal van een device waar zakelijke mail op aanwezig is dient direct bij de supportdesk van de afdeling ICT gemeld te worden.
- Direct na uitdiensttreding dienen medewerkers de zakelijke mail van hun privé device(s) te verwijderen.

Randvoorwaarden en verantwoordelijkheden ziekenhuis zijn:

- Bij melding van verlies/diefstal van het device zal een medewerker van afdeling ICT de zakelijke mail faciliteit zo snel als mogelijk blokkeren.

Gebruikersnaam / wachtwoorden

De gebruiker heeft toegang tot de ICT-voorzieningen door middel van een gebruikersnaam, wachtwoord en eventueel een code via MFA. De regels rondom toegang en authenticatie zijn beschreven in Gebruikerstoegang en authenticatie: informatieveiligheid (versie 1) (iprova.nl).

Het wachtwoord dient regelmatig te worden gewijzigd. Het moment van wijziging wordt getoond bij het inloggen.

Het is niet toegestaan om gebruikersnamen en wachtwoorden van systemen van het Dijklander Ziekenhuis:

- Aan derden beschikbaar te stellen (met derden worden tevens andere medewerkers van het Dijklander Ziekenhuis bedoeld).
- Op een voor anderen of openbaar toegankelijke plek of anderszins onzorgvuldig te bewaren.
- Van andere medewerkers op enigerlei wijze en in enigerlei vorm te bemachtigen en/of te gebruiken.
- Voor sites of apps buiten het Dijklander Ziekenhuis te gebruiken. Als ze buiten gevonden of gestolen worden, kunnen ze binnen gebruikt worden.
- Op te slaan of te programmeren in scripts of onder een functietoets.

De medewerker dient de combinatie gebruikersnaam en wachtwoord(en) zorgvuldig te beheren. De medewerker blijft verantwoordelijk voor zijn/haar eigen wachtwoordgebruik.

Het is van belang dat wachtwoorden geheim blijven. Daarom is het niet handig om wachtwoorden op te schrijven (of je moet ze heel goed verstoppen). Wachtwoorden kunnen in een datakluis worden bewaard, hiervoor zijn apps beschikbaar, zoals KeePass, LastPass.

De medewerker dient zijn wachtwoorden direct te veranderen als hij vermoedt dat iemand die heeft kunnen zien of als hij vermoedt dat ze niet langer geheim zijn. Lukt dit niet, dan neemt hij zo snel mogelijk contact op met de helpdesk ICT.

Privégebruik op of via zakelijke ICT-middelen (werkplek, e-mail, internet)

Op de computer of de laptop die door het Dijklander Ziekenhuis beschikbaar wordt gesteld, is een beveiligde, werk gerelateerde omgeving ingericht. Privégebruik van ICT-middelen is beperkt toegestaan, mits dit geen belemmering inhoudt voor de dagelijkse werkzaamheden of extra belastend is voor het computernetwerk.

Om de privacy te waarborgen, is het van belang dat privébestanden, -berichten en dergelijke duidelijk van werk gerelateerde informatie gescheiden worden gehouden. Dit wordt gedaan door deze apart in mappen met “Privé” in de naam op te slaan. Het Dijklander Ziekenhuis zal het privékarakter van digitale persoonlijke bestanden van personeelsleden respecteren en mag niet zonder meer toegang krijgen daartoe. In bijzondere omstandigheden kan de werkgever toegang aanvragen.

Het automatisch doorsturen van berichten die binnenkomen op het zakelijk e-mail account, naar een privé e-mailadres is niet toegestaan. De medewerker dan immers niet controleren of er vertrouwelijke informatie tussen zit.

Wees alert en stuur geen vertrouwelijke informatie naar het privé e-mailadres.

Het zakelijke e-mailadres is bedoeld voor zakelijk gebruik. Het is toegestaan om met het zakelijke e-mailadres in te schrijven op nieuwsbrieven van een zakelijk karakter en/of doel, wel met het advies om dit tot een minimum te beperken. Het is niet toegestaan om het zakelijk e-mailadres te gebruiken voor het aanmelden voor het reageren op reclame en ander niet zakelijke doeleinden. Zo draagt iedere medewerker bij aan het voorkomen van spam.

Financiële transacties voor privédoeleinden zijn niet toegestaan op of via ICT-middelen. Dit omvat commerciële activiteiten, zoals bestellingen en boekingen, beurshandel, gokken of spelletjes met financiële verrekening of betaalde telefoondiensten. Een uitzondering is internetbankieren via een beveiligde verbinding met zijn/haar bank.
NB: de medewerker controleert te allen tijde of de verbinding beveiligd is door het slotje en de groene adresbalk.

Mobiel veilig werken

Het werken met een laptop van het Dijklander Ziekenhuis thuis en onderweg is beveiligd. Bij het inloggen op het account wordt een beveiligde verbinding gemaakt. Werken met e-mail op de eigen telefoon of tablet is beveiligd, maar de medewerker dient bij op het openen van bijlagen en documenten, op de telefoon, tablet of (eigen of openbare) computer alert te zijn op risico’s. De kans bestaat dat er spam of phishingmail in de mailbox terechtkomt. Deze kunnen mogelijk indirect ICT-middelen van het Dijklander Ziekenhuis besmetten of misbruiken bij het openen van deze mail.

Medewerkers zullen Bluetooth, GPS en personal hotspot op de telefoon standaard uitzetten. Hierdoor wordt de smartphone of tablet extra kwetsbaar.

Gebruik is toegestaan wanneer het echt nodig is en alleen wanneer het mogelijk is om in een veilige omgeving te werken.

Werken met Wi-Fi

De medewerker gebruikt standaard zijn 4G of 5G-verbinding voor internet-toegang buiten de deur.

De medewerker is voorzichtig met het gebruik van Wi-Fi, zowel met zijn eigen apparatuur als met apparatuur die van het Dijklander Ziekenhuis is ontvangen. Gratis Wi-Fi, zoals vaak aanwezig is in hotels en op vliegvelden en soms in horecagelegenheden, is veelal onbeveiligd. Ook al wordt een (tijdelijke) Wi-Fi-code verstrekt of verkocht, het berichtenverkeer via die Wi-Fi-verbinding kan door onbevoegden worden afgevangen en toegankelijk worden gemaakt.

Werken met eigen apparatuur

Werken met eigen apparatuur is toegestaan, mits er op de digitale werkomgeving van Dijklander Ziekenhuis wordt gewerkt én geen informatie van het Dijklander Ziekenhuis op de eigen apparatuur wordt opgeslagen.
Hieraan worden de volgende eisen gesteld:

- De gebruikte apparatuur moet voorzien zijn van een 2FA oplossing of Biometrische beveiliging.
- De gebruikte apparatuur dient te zijn voorzien van de laatste updates-patches.
- De gebruikte apparatuur dient te zijn versleuteld.
- De gebruikte apparatuur dient indien mogelijk te zijn voorzien van Anti-virus/malware oplossing.

In dit verband wordt er ook verwezen naar de regels over veilig opslaan van bedrijfsinformatie in het document ‘aanvaardbaar gebruik van bedrijfsmiddelen’ (in ontwikkeling).

Apps op een tablet of smartphone

Op de van het Dijklander Ziekenhuis ontvangen laptop en smartphone is het toegestaan om apps uit de normale app-store te downloaden. Medewerker dient zich ervan bewust te zijn dat sommige apps gebruik maken van in-app aankopen, die ongemerkt tot hoge kosten kunnen leiden. De kosten voor het aanschaffen en gebruiken van de apps zijn voor eigen rekening.

Medewerker dient zich ervan bewust te zijn van de rechten die een app vraagt en dient hier verstandig mee om te gaan. De rechten dienen zo beperkend mogelijk te worden ingesteld. Veel apps vragen om meer rechten dan nodig zijn voor het goed functioneren. Voorbeelden zijn toegang tot contact- of andere privégegevens of rechten om je account of draadloze verbinding te gebruiken. Dit biedt mogelijkheden tot misbruik: dergelijke apps zijn een bekende bron van virussen en malafide software.

De medewerker kan bij elk twijfel contact opnemen met ICT Service Punt.

Het inbreken op de smartphone of tablet van het Dijklander Ziekenhuis, om op die wijze gebruik te kunnen maken van applicaties die niet in de reguliere app-stores te verkrijgen zijn, is niet toegestaan.

Social media, blogs, wiki’s, fora en andere media

Voor de omgang met social media en je gedrag in de Samenwerkingsfunctionaliteit geldt het “Social media: Gedragscode / Omgaan met social media voor werknemers”. De medewerker is altijd zorgvuldig, betrouwbaar, integer en respectvol in zijn uitlatingen.

Medewerkers moeten alle informatie vanuit het Dijklander Ziekenhuis beschouwen als vertrouwelijk tenzij uitdrukkelijk anders is bepaald.

Medewerkers zijn persoonlijk verantwoordelijk voor de inhoud die ze - voor zover dat niet tot hun functie behoort - publiceren op social media, blogs, wiki’s, fora (zoals Facebook, LinkedIn, Snapchat, Twitter en Instagram) en andere media die gebaseerd zijn op user-generated content (= door gebruiker gemaakte inhoud)

Medewerkers zijn zich ervan bewust dat wat zij (privé) publiceren voor langere tijd openbaar zal worden, hetgeen mogelijk gevolgen kan hebben voor hun werksituatie. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- Over privacygevoelige en/of bedrijfsgevoelige informatie, waaronder patiëntengegevens, financiële gegevens en bijvoorbeeld incidenten en calamiteiten, wordt niet gepubliceerd.
- Medewerkers van het Dijklander Ziekenhuis respecteren degene tot wie zij zich richten binnen en buiten de werksituatie.
- Etnische laster, persoonlijke beledigingen en obsceniteit zijn niet geoorloofd. De privacy van anderen wordt gerespecteerd en de reputatie van het ziekenhuis wordt niet geschaad.
- Medewerkers die publiceren op een website anders dan die van het Dijklander Ziekenhuis over een onderwerp dat wel te maken kan hebben met het Dijklander Ziekenhuis, maken kenbaar dat zij op persoonlijke titel publiceren.
- Blogs en sociale netwerken die worden gehost door het Dijklander Ziekenhuis moeten worden gebruikt op een manier die waarde toevoegt aan de bedrijfsdoelstellingen en het imago van het Dijklander Ziekenhuis.
- Het maken van een selfie is toegestaan, mits dit de werkzaamheden niet hindert, niemand in beeld brengt die dat niet wenst en de privacy van anderen dan wel de reputatie van het ziekenhuis niet schaadt.

Gebruik Whatsapp

Medewerkers mogen Whatsapp gebruiken om met collega's afstemming te hebben, bijvoorbeeld over hun rooster. Het delen van herleidbare foto's, beelden of gegevens van patiënten via Whatsapp is expliciet niet toegestaan. Whatsapp wordt hiervoor niet als voldoende veilig beschouwd.
Alleen als de informatie voor de ontvanger niet herleidbaar is tot een identificeerbare patiënt (bijvoorbeeld als er geen patiëntnaam wordt genoemd), dan is de privacy niet in het geding en mag WhatsApp wél gebruikt worden. Maar zorgvuldig handelen hierbij blijft noodzakelijk.

Als alternatief voor Whatsapp heeft het ziekenhuis een veilig app aangekocht: Siilo. De applicatie is te gebruiken op IOS- & Androidapparaten (https://www.siilo.com/nl/). Voor communicatie via Siilo geldt dat er geen belemmeringen zijn met betrekking tot het delen van informatie: er kunnen dus gerust (herleidbare) patiëntgegevens worden uitgewisseld via Siilo.

Telefonie

Medewerkers mogen incidenteel en kortstondig de telefoon voorzieningen van het Dijklander Ziekenhuis gebruiken voor het voeren van privégesprekken, mits dit geen storende onderbreking vormt van de werkzaamheden en mits hierbij voldaan wordt aan de verdere richtlijnen van deze gedragscode.

Het is medewerkers in ieder geval verboden telefoons van het Dijklander Ziekenhuis te gebruiken om:
- Servicenummers te bellen die beginnen met 0906 en 0909 anders dan voor doeleinden die voortvloeien uit de functie;
- Internationale nummers te bellen voor privédoeleinden;
- Uitgaande telefoongesprekken te voeren die inhoudelijk strijdig zijn met wet- en regelgeving en de goede naam van het Dijklander Ziekenhuis op het spel zetten.

Medewerkers dienen zich ervan bewust te zijn dat een mobiele telefoon veel informatie kan bevatten waardoor de privacy van medewerkers en de patiënt in het geding kunnen komen. Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:
- Het toestel zodanig bij zich dragen dat diefstal of verlies wordt voorkomen.
- In beginsel is het niet toegestaan om vertrouwelijke (persoons)gegevens en/of bedrijfsgevoelige informatie (zoals e-mail) op de telefoon op te slaan en wanneer dit wel voor het uitoefenen van de functie noodzakelijk is dienen de gegevens zodanig te worden versleuteld dat de privacy blijft gewaarborgd. Dit geldt tevens voor foto-, video- en geluidsopnames.
- Indien de mobiele telefoon vertrouwelijke gegevens/persoonsgegevens en/of bedrijfsgevoelige informatie bevat dient het bij vermissing of diefstal direct als veiligheidsincident te worden gemeld bij de IT Servicedesk.

Gebruik werkstations

- Gevoelige bedrijfsinformatie en patiëntgegevens mogen uitsluitend op de netwerkschijf worden opgeslagen. Van deze, op de server geplaatste bestanden, maakt de ICT-afdeling volgens vastgestelde procedures back-ups.
- De medewerker die besluit bestanden op de lokale C-schijf op te slaan, is persoonlijk verantwoordelijk voor het beheer van deze bestanden. Van betreffende bestanden wordt door de afdeling ICT geen back-up gemaakt.
- De medewerker is zelf verantwoordelijk voor de inhoud van de door hem/haar zelf geproduceerde bestanden. Het ziekenhuis draagt geen verantwoordelijkheid.
- De medewerker dient de ter beschikking gestelde ICT-apparatuur te gebruiken conform de voorschriften en/of aanwijzingen van medewerkers van de afdeling ICT.
- Apparatuur die onder verantwoording van ICT valt, mag alleen worden verplaatst door medewerkers van de afdeling ICT of door medewerkers na overleg en met toestemming van de supportdesk medewerker ICT.
- De medewerker mag de netwerkaansluitingen (kabels) niet zelf wijzigen.
- De medewerker dient aanwijzingen ten aanzien van beveiliging, zoals virusbestrijding, op te volgen.
- Incidenten die het normale gebruik van de voorzieningen verstoren dient de medewerker terstond aan de supportdesk ICT te melden.

Mobiele gegevensdragers

Dossiers, papieren, DVD's, USB-memorysticks, laptops, notebooks, tablets en overige informatiedragers die vertrouwelijke (persoons)gegevens en/of bedrijfsgevoelige informatie bevatten, dienen met de grootst mogelijke zorgvuldigheid te worden bewaard. Het is in ieder geval niet toegestaan om opgeslagen bestanden op mobiele gegevensdragers die privacygevoelige informatie bevatten onbeheerd achter te laten, of niet goed genoeg te beschermen tegen verlies of diefstal.

Indien de mobiele gegevensdrager vertrouwelijke gegevens/ persoonsgegevens en/of bedrijfsgevoelige informatie bevat, dient dit bij vermissing of diefstal direct als veiligheidsincident gemeld te worden bij de IT Servicedesk.

Toegang tot informatie en informatie verwerkende systemen

Bij indiensttreding ontvangt de medewerker toegang (een inlogaccount) tot het netwerk en een basis-reeks aan informatievoorzieningen. De functie en het soort informatie waarmee de medewerker werkt, is daarbij bepalend voor welke aanvullende informatievoorzieningen nodig zijn voor zijn functie-uitoefening. Op basis van de functie van de medewerker al dan niet in combinatie met de organisatorische eenheid en werklocatie, wordt op basis van de autorisatiematrix bepaald welke toegangsrechten en voorzieningen een medewerker krijgt.

Het is nooit toegestaan om de inloggegevens of een openstaande sessie van een collega te gebruiken.

Soms is het nodig, bijvoorbeeld voor de continuïteit van de werkzaamheden, dat collega's bij e-mail en bestanden van een niet aanwezige medewerker kunnen. In overleg met de leidinggevende kan de medewerker een collega digitaal machtigen om onder zijn account binnengekomen berichten te raadplegen, onder de afspraak dat het eventuele privékarakter gerespecteerd wordt. De collega kan bij overtreding van die afspraak disciplinair aangesproken worden. Het is verstandig om hiervoor een gedeelde account te gebruiken, waarop een ieder via zijn eigen account inlogt.

Authenticatiemiddelen

Wachtwoorden, tokens en pasjes voor toegang tot informatiediensten en ruimtes worden aan een medewerker verstrekt voor persoonlijk gebruik. Daarmee bewijst degene on- en offline dat hij degene is die hij beweert te zijn. Bij ontvangst van de middelen ondertekent de medewerker een gebruikersovereenkomst waarin de rechten en plichten staan vermeld.

Naast een wachtwoord of PIN(code) (dat je weet) gebruikt het Dijklander Ziekenhuis een 2e factor: iets dat de medewerker bezit (een token, smartphone, pasje of certificaat).

De medewerker geeft zijn wachtwoord, pasje of token nooit aan anderen; ook niet aan IT-beheerders!

Clear desk & clear screen

Als de medewerker even niet op zijn werkplek is dient hij de ICT-middelen te vergrendelen (bijvoorbeeld met CTRL-ALT-DEL of door pas op paslezer te leggen voor je beeldscherm of door het apparaat uit te schakelen) zodat er geen misbruik van gemaakt kan worden.

Alvorens weg te lopen van de werkplek worden ook alle vertrouwelijke papieren in een lade of kast opgesloten. Het document Clear desk & clear screen: Beleid (versie 6) (iprova.nl) beschrijft de regels binnen Dijklander Ziekenhuis.

Omgang met vertrouwelijke informatie

Een medewerker heeft vaak toegang tot een veelheid aan informatie, waaronder vertrouwelijke of gevoelige informatie. Informatie kan bijvoorbeeld privacygevoelig of personeelsvertrouwelijk zijn. Met al deze informatie moet op zorgvuldige wijze worden omgegaan.

Medewerkers maken gebruik van de middelen die aan hen worden aangereikt om de toegang beveiligen.

Informatie (en vooral informatie over personen) wordt alleen gebruikt voor het doel waarvoor die aan Dijklander Ziekenhuis is verstrekt en vertrouwelijke informatie mag niet met onbevoegden worden gedeeld.

Het verwerken van gevoelige of vertrouwelijke informatie op onveilige apparatuur (privémiddelen of voorzieningen in bijvoorbeeld openbare ruimtes) is risicovol en is dan ook niet toegestaan.

Voor het gebruik van het EPD geldt de Gedragscode: Gedragscode: gebruik en inzage van het Elektronisch Patiënten Dossier (EPD) (versie 9) (iprova.nl).

Verlies of diefstal van persoonsgegevens: datalek

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we mogelijk van een datalek in het kader van de Algemene Verordening Gegevensbescherming. Denk hierbij aan uitgelekte computerbestanden, gestolen of verloren datadragers waarop persoonsgegevens staan of wanneer bij een (digitale)inbraak dossiers met gegevens over personen (mogelijk) zijn ingezien door derden.

Bij verlies van een informatie(dragers), inbraak of diefstal, wordt dit direct gemeld bij de helpdesk ICT.
Daarnaast wordt ook direct een datalekmelding gedaan, via Zenya | Meldingen - Datalek (iprova.nl).

De medewerker dient ook aangifte te doen bij de politie en een kopie van het proces-verbaal aan de Privacy Officer te verstrekken.

Respecteer andermans eigendommen

Medewerker van het Dijklander Ziekenhuis respecteren de auteursrechten en (intellectuele)eigendomsrechten van anderen. Soms is een bronvermelding onvoldoende. Wanneer bestanden en informatie ten behoeve van de werkzaamheden van het internet worden gedownload controleert de medewerker altijd of op de site expliciet wordt vermeld dat downloaden (wettelijk) is toegestaan, Het downloaden van auteursrechtelijk beschermde foto's, muziek- en filmbestanden mag niet zonder toestemming van de eigenaar en is strafbaar.

Hulpmiddelen voor toegang tot locaties

Medewerkers gebruiken de hulpmiddelen voor toegang tot locaties, apparatuur en ruimten van het Dijklander Ziekenhuis (zoals sleutels en pasjes) uitsluitend voor het doel waarvoor deze ter beschikking zijn gesteld.

Medewerkers worden geacht hier met alle mogelijke voorzichtigheid mee om te gaan en in ieder geval de volgende zaken in acht te nemen:

- De medewerker probeert niet om onbevoegd toegang te krijgen tot locaties van het Dijklander Ziekenhuis.
- Voor de medewerker bestemde toegangsmiddelen zijn uitsluitend bedoeld voor persoonlijk gebruik en mogen niet beschikbaar worden gesteld aan collega's of andere derden, tenzij daarover andere schriftelijke afspraken zijn gemaakt met de leidinggevende en/of het Facilitair Servicepunt.
- Bij vermissing, ontvreemding, misbruik of ander onrechtmatig gebruik van personeelspas, sleutels, tags, toegangscodes, apparatuur of software stelt de medewerker de leidinggevende en het Facilitair Servicepunt onmiddellijk op de hoogte.

Privacy

Medewerkers dienen alle mogelijke middelen aan te wenden om de privacy van patiënten en van andere medewerkers te waarborgen. Aan derden worden geen gegevens over patiënten verstrekt, tenzij dit noodzakelijk is voor de behandeling of aan de door patiënt aangewezen contactpersoon. In dat laatste geval is uitdrukkelijke toestemming nodig van betrokken patiënt.

Over medewerkers worden geen gegevens verstrekt aan derden of andere medewerkers. Vragen over medewerkers worden doorverwezen naar de HR-afdeling.

Om de privacy van de patiënten van het Dijklander Ziekenhuis te kunnen waarborgen, is het niet toegestaan om foto-, film- of geluidsopnamen te maken in het Dijklander Ziekenhuis en op het terrein van het Dijklander Ziekenhuis zonder uitdrukkelijke toestemming van de daartoe bevoegde personen in het Dijklander Ziekenhuis alsmede de betreffende patiënt(en). Onder opname wordt verstaan alle vormen van geluid- en/of beeldregistratie.

Melden van incidenten (inclusief datalekken) en kwetsbaarheden

Medewerkers dienen alle mogelijke middelen aan te wenden om de privacy van patiënten en van andere medewerkers te waarborgen.

Medewerkers zijn medeverantwoordelijk voor de betrouwbaarheid en weerbaarheid van de informatievoorziening van het Dijklander Ziekenhuis. Daarom wordt van hen veilig en integer handelen verwacht. Daarbij hoort ook dat zij alert zijn en zaken signaleren. Wanneer de medewerker iets afwijkends opmerkt of iets niet vertrouwt, dient de medewerker dit te melden als een incident:

- Technische incidenten (bijvoorbeeld een virus): meld dit bij de helpdesk ICT;
- Een kwetsbaarheid in ICT-middelen: meld dit bij de helpdesk ICT als (mogelijk) beveiligingsincident.
- Overige incidenten (bij diefstal, verlies of een fout bij het verzenden/delen van een bericht of bestand): als vertrouwelijke of persoons-informatie (mogelijk) in handen is gekomen van onbevoegden, meld dit direct bij je leidinggevende en via Zenya als (mogelijk) datalek via Zenya | Meldingen - Datalek (iprova.nl);
- Een verdacht bericht (bijvoorbeeld vermoeden van phishing of aanstootgevende inhoud): informeer je leidinggevende of vraag advies aan de CISO of FG als je de inhoud van een bericht of de werking van een programma niet vertrouwt.

De registratie van de melding gebeurt primair om de kwaliteit van de zorg te verbeteren en om het beheer, de continuïteit, de veiligheid, de integriteit en de beschikbaarheid van de infrastructuur en de diensten te waarborgen, alsmede om verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan.

Monitoring en controle

Van alle medewerkers wordt verwacht dat zij zich actief inspannen om informatie(systemen) te beveiligen in het eigen belang en in het belang van het ziekenhuis.
Informatiebeveiliging is een integraal onderdeel van de normale werkzaamheden en een kwaliteitsaspect waarmee de medewerker voortdurend rekening moet houden gedurende werktijd.
Binnenkomend internet- en e-mailverkeer wordt zo goed mogelijk gecontroleerd op virussen, spam en soortgelijk ongerief.

Mocht blijken dat een e-mailbericht een virus bevat, dan wordt het automatisch tegengehouden en worden de verzender en ontvanger daarover ingelicht. Indien desondanks materiaal wordt ontvangen dat mogelijk een virus bevat, dan dient de ontvanger onverwijld contact op te nemen met de supportdesk ICT en het te melden als veiligheidsincident. De ontvanger onthoudt zich ervan om zelf verder enige actie te ondernemen, zodat verspreiding van het virus wordt voorkomen.

Het gebruik van internet- en e-mailverkeer kan door het Dijklander Ziekenhuis worden gemonitord. Deze registratie gebeurt om het beheer, de continuïteit, de veiligheid, de integriteit en de beschikbaarheid van de infrastructuur en de diensten te waarborgen, verstoring van bedrijfsprocessen en andere (financiële) schade tegen te gaan en om toezicht te houden op de naleving van de gedrags- en gebruiksregels binnen het ziekenhuis.

Inbreuk op de gedragscode

Het overtreden van de regels met betrekking tot deze Gedragscode wordt als een plichtsverzuim beschouwd. Afhankelijk van de aard en ernst van het vastgestelde plichtsverzuim kan dit verschillende sancties en maatregelen tot gevolg hebben. Hierbij wordt verwezen naar het document Sancties: bij overtredingen inzake informatieveiligheid (versie 2) (iprova.nl).

Bij ernstige inbreuk op deze Gedragscode zal de raad van bestuur op de hoogte worden gesteld.

Bewustwording

Om het bewustzijn voor informatiebeveiliging niet te verliezen wordt het onderwerp regelmatig onder de aandacht gebracht bij de medewerkers. Hierbij wordt verwezen naar het NEN7510: Opleidingsplan privacy en informatiebeveiliging 2024 (versie 1) (iprova.nl) en het 'NEN7510: Communicatieplan privacy en informatiebeveiliging (ISMS - H0.7) (versie 1) (iprova.nl).

Uitzonderingen
Indien er zich situaties voordoen waarin deze Gedragscode niet voorziet, zal conform het arbeidsrechtelijk kader worden gehandeld.

Werking

Deze Gedragscode bepaalt het minimumkader dat in het Dijklander Ziekenhuis van toepassing is. Met de inwerkingtreding van deze Gedragscode vervallen de bestaande/oudere regelingen van het Dijklander Ziekenhuis en treedt deze regeling daarvoor in de plaats.

Vaststelling, uitvoering en beheer

Dit document is vastgesteld door Raad van Bestuur en wordt voor uitvoering bekend gemaakt aan alle medewerkers.

De CISO houdt toezicht op de toepassing en werking van dit tactisch beleid. Revisie en aanvulling is een doorlopende (maar tenminste jaarlijkse) verantwoordelijkheid van de CISO. Wijzigingen leiden tot opnieuw vaststellen van een nieuwe versie van dit document.

Werkwijze

Regels voor het zorgvuldig gebruik van voorzieningen

Veiligheid: risicomomenten en te ondernemen acties

Het niet naleven van deze gedragscode kan o.a. schade berokkenen aan de privacy van de patiënt, o.a. resulterend in klachten en claims van patiënten, maatregelen van de IGZ, het verliezen van de NIAZ-accreditatie en imagoschade voor het Dijklander Ziekenhuis.

Daarnaast kan niet naleven van deze gedragscode leiden tot een verhoogd risico op uitval van informatiesystemen, met risico's voor de patiënt en de continuïteit van de bedrijfsvoering als gevolg.

Samenhangende documenten

Dijklander gedragscode : #zodoendijklanders (versie 1) (iprova.nl)
NEN7510: ISMS - H0.5 - Informatiebeveiligingsbeleid (versie 3) (iprova.nl)
NEN7510: Privacybeleid (versie 3) (iprova.nl)
Sancties: bij overtredingen inzake informatieveiligheid (versie 2) (iprova.nl)
Gedragscode: gebruik en inzage van het Elektronisch Patiënten Dossier (EPD) (versie 9) (iprova.nl)
NEN7510: Opleidingsplan privacy en informatiebeveiliging 2024 (versie 1) (iprova.nl)
NEN7510: Communicatieplan privacy en informatiebeveiliging (ISMS - H0.7) (versie 1) (iprova.nl)
Social media: Gedragscode / Omgaan met social media voor werknemers (versie 2) (iprova.nl)
Zenya | Meldingen - Datalek (iprova.nl)