ICT Protocol

Versie: 2.0

Vertrouwelijkheidsniveau: Betrokkenen

GVB Door en door Amsterdam

Inleiding

Dit ICT Protocol geeft de regels voor het gebruik van ICT middelen en diensten door medewerkers van GVB. Dit geldt voor zowel de middelen en diensten die door GVB ter beschikking worden gesteld als niet door GVB ter beschikking gestelde ICT-middelen en ICT-diensten. Ook lees je in dit protocol de manier waarop controle en toezicht wordt gehouden.
Voor medewerkers in dienst van GVB is dit ICT-Protocol van toepassing. Dit is bepaald in de cao GVB (artikel 15.17). De cao wordt van toepassing verklaard op de medewerker in de arbeidsovereenkomst.
Voor personen die door GVB worden ingehuurd wordt het ICT Protocol getekend bij aanvaarding van de opdracht. Daardoor is het een onderdeel van de inhuurovereenkomst.
Het ICT Protocol is tot stand gekomen met instemming van de OR.

Definities	
Medewerker	iedere persoon in dienst van GVB en personen die door GVB worden ingehuurd om werkzaamheden voor GVB te verrichten.
ICT-middelen	hardware, software en netwerkfaciliteiten, waaronder – maar niet uitsluitend – internet, e-mail, telefoon, computer- en randapparatuur in de ruimste zin van het woord. We maken in dit Protocol een onderscheid tussen door GVB ter beschikking gestelde ICT-Middelen en ICT-Middelen die niet door GVB ter beschikking zijn gesteld.
ICT-diensten	processen en diensten, zoals digitale opslag en digitale rekenkracht, apps en web applicaties, die door externe partijen beschikbaar zijn gesteld om te gebruiken door GVB of door medewerker en voor door GVB bepaalde doeleinden gebruikt worden.
Bedrijfsgegevens	alle gegevens waarvoor GVB verantwoordelijk is en op aangesproken kan worden indien daar onrechtmatig en/of onzorgvuldig mee wordt omgegaan.
GVB	GVB Holding N.V. en de daaraan gelieerde ondernemingen, gevestigd aan de Arlandaweg 106 te Amsterdam en ingeschreven in de Kamer van Koophandel onder nummer 34258789.
Beheerder (afdeling ICT&I)	degene die binnen GVB of buiten GVB in opdracht van GVB verantwoordelijk is voor het goed laten functioneren van ICT-middelen en ICT-diensten.
Compliance officer	De functionaris die bewaakt of een bedrijf en de medewerkers zich houden aan de regels voor onder andere goed bestuur, gedrag en integriteit.
Datalek	een inbreuk op de beveiliging die per ongeluk of op onrechtmatige wijze leidt tot de vernietiging, het verlies, de wijziging of ongeoorloofde toegang tot gegevens.
Functionaris gegevensbescherming	degene die bij GVB toezicht houdt op de toepassing en naleving van de Algemene verordening gegevensbescherming (AVG). Dit is ook degene die op de hoogte gesteld moet worden als persoonsgegevens ongeautoriseerd buiten GVB zijn beland.

1 Algemene uitgangspunten

1.1 Algemeen gebruik

Voor medewerkers bij GVB is gebruik van ICT-middelen en ICT-diensten nodig om de werkzaamheden goed uit te voeren. Onjuiste omgang met ICT-middelen of misbruik kost tijd en capaciteit van personen en apparatuur en brengt verschillende risico's met zich mee. Bovendien bestaat het risico op het in strijd handelen met wet- en regelgeving en op beveiligingsincidenten, zoals datalekken.

1.2 Handelen van de medewerker

GVB verwacht van de medewerker professioneel, integer en zorgvuldig handelen.

1.3 Gebruik van niet door GVB ter beschikking gestelde ICT-middelen

Bedrijfs- en persoonsgegevens zijn toegankelijk met ICT-middelen en ICT-diensten die door GVB ter beschikking zijn gesteld. GVB staat het gebruik van niet door GVB ter beschikking gestelde ICT-middelen privé ICT-middelen voor zakelijk gebruik toe, als er geen bedrijfs- en persoonsgegevens op die privé-middelen worden opgeslagen. De niet door GVB ter beschikking gestelde ICT-middelen worden niet door GVB onderhouden. De medewerker zorgt er zelf voor dat het ICT-middel waarmee wordt gewerkt veilig is.

1.4 Niet openbare bedrijfsgegevens

Alle niet openbare bedrijfsgegevens blijven binnen de ICT-middelen en ICT-diensten van GVB. Als het voor de taakuitoefening nodig is kunnen medewerkers GVB-bedrijfsgegevens uitwisselen met zakelijke partners van GVB. Deze gegevens mogen geen persoonsgegevens bevatten. In het laatste geval kan het uitsluitend als daarvoor afspraken worden gemaakt met de ontvangende partij. Onder meer over het gebruik van de gegevens, de beveiliging, de vernietiging na gebruik en wat te doen in geval van een datalek. Mogelijk is een verwerkersovereenkomst noodzakelijk. Omdat de feitelijke omstandigheden bepalend zijn, is de beoordeling maatwerk en moet contact worden opgenomen met het Privacy Office.

1.5 Inloggegevens en authenticatiemiddelen

Met persoonlijk toegekende inloggegevens, aanvullende authenticatiemiddelen (zoals smartcards en tokens) en overige beveiligingshulpmiddelen moet zorgvuldig worden omgegaan. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld.

1.6 Privégebruik van ICT-middelen

Privégebruik van ICT-middelen onder werktijd is incidenteel toegestaan, onder de voorwaarde dat dit niet storend is voor of ten koste gaat van het uitvoeren van de dagelijkse werkzaamheden. Het is vanzelfsprekend dat privégebruik onder werktijd in overeenstemming is met dit ICT-Protocol.

2 ICT-middelen en ICT-diensten die door GVB ter beschikking zijn gesteld

2.1 Beperking websites en telefoonnummers

GVB kan de toegang tot niet-functionele websites of de toegang tot bepaalde telefoonnummers beperken.

2.2 Regels digitale communicatie

De regels die gelden voor het ondertekenen van schriftelijke correspondenties, correct taalgebruik, het vertegenwoordigen van GVB en het verzenden van post zijn ook van toepassing op e-mail en andere vormen van elektronisch berichtenuitwisseling.

2.3 Regels voor het gebruik van ICT-middelen

GVB verwacht dat de medewerker professioneel, integer en zorgvuldig handelt. Het is niet toegestaan om:

a. websites te bezoeken die pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten. Het is ook niet toegestaan dergelijk materiaal te downloaden;
b. zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet (hacken);
c. informatie waartoe via internet toegang is verkregen opzettelijk en zonder toestemming te veranderen of te vernietigen (vorm van hacken);
d. bestanden op te slaan buiten de GVB omgeving;
e. films, muziek, applicaties en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron;
f. berichten te versturen aan een groot aantal ontvangers. Het versturen van een bericht of e-mail aan ‘Alle gebruikers’ mag uitsluitend alleen met toestemming van de bevoegd leidinggevende en het hoofd ICT.
g. dreigende, beledigende, aanstootgevende, seksueel getinte, racistische, discriminerende berichten of kettingmailbrieven te verzenden of door te sturen;
h. iemand elektronisch lastig te vallen.

Als de medewerker ongevraagd informatie van deze aard aangeboden krijgt, meldt de medewerker dit direct aan de leidinggevende.

2.4 Twijfel over regels

Bij twijfel over de betekenis van de in 2.3 genoemde regels kan de medewerker contact opnemen met de leidinggevende. Mocht dat gezien de situatie niet wenselijk zijn, dan kan contact worden opgenomen met het Meldpunt Integriteit. In de cao GVB staat een gedragslijn vermoeden van misstanden (Hoofdstuk 21).

2.5 Recht tot gebruik intrekken

GVB kan het recht tot gebruik van door GVB ter beschikking gestelde ICT-middelen en ICT-diensten toestaan en ook weer intrekken. Zonder dat recht is gebruik van door GVB ter beschikking gestelde ICT-middelen en ICT-diensten niet toegestaan.
Alle zakelijk beschikbaar gestelde ICT-middelen, alsmede alle door GVB ter beschikking gestelde gegevens blijven te allen tijde eigendom van GVB.

2.6 Storing bij ICT-middelen

Wanneer ICT-middelen niet functioneren vanwege een (technische) storing dan is de Servicedesk ICT het eerste aanspreekpunt. De Servicedesk ICT is te bereiken op servicedeskict@gvb.nl of telefonisch op 088-6500015.

2.7 Toegang tot ter beschikking gestelde ICT-middelen

Als de medewerker vanwege bijzondere omstandigheden een langere tijd niet in staat is om zich toegang te verschaffen tot door GVB ter beschikking gestelde ICT-middelen, bijvoorbeeld vanwege langdurige arbeidsongeschiktheid of onbereikbaarheid van de medewerker, dan is GVB gerechtigd de beheerder op verzoek van de leidinggevende daartoe toegang te geven. Dat kan alleen als er sprake is van een zwaarwegend bedrijfsbelang én als de medewerker hiervan op de hoogte is gesteld.
De beheerder mag zich geen toegang geven tot niet door GVB ter beschikking gestelde gemarkeerde mappen, bestanden of (mail)folders.

De volgende stappen worden gevolgd bij toegang geven tot de door GVB ter beschikking gestelde ICT-middelen:

1. De leidinggevende van de betreffende (oud-)medewerker dient een verzoek in bij de ICT Servicedesk. De leidinggevende geeft daarbij aan waaruit het zwaarwegend belang van GVB bestaat, en specificeert op welke documenten, e-mails etc. het verzoek betrekking heeft.
2. De ICT Servicedesk legt het verzoek voor aan de directeur HR (of diens plaatsvervanger in geval van afwezigheid), die namens GVB besluit over het verzoek. De toegang wordt alleen verleend als er geen andere mogelijkheid is om de gevraagde documenten terug te vinden.
3. De toegang wordt verleend aan de directeur ICT & Innovatie, die gericht zoekt naar de gespecificeerde documenten. Voordat gezocht wordt naar bestanden zal GVB door inschakeling van een vertrouwenspersoon de computer van medewerker controleren om zo privémails en -bestanden te herkennen en in een aparte map te plaatsen.
4. Direct nadat de verzochte documenten zijn opgeleverd aan de verzoeker, wordt de toegang weer ingetrokken.
5. De opgeleverde documenten worden conform hun normale bewaartermijn vernietigd.

3 Thuis of op locatie werken

3.1 Inloggen buiten GVB netwerk

De medewerker logt buiten kantoor (bijvoorbeeld thuis) in via de thuiswerkportal (Citrix Portal) of Office365. Daarmee wordt de veiligheid van de informatie gewaarborgd.

3.2 Thuiswerken

Thuiswerken doet de medewerker via de thuiswerkportal. Het (versimpelde) stappenplan is als volgt:

1. De thuiswerkportal is te bereiken via ci.gvb.nl.
2. De medewerker krijgt (eenmalig) een verzoek om de Citrix Workspace te installeren.
3. Vervolgens logt medewerker met de GVB gebruikersnaam en wachtwoord in en selecteert in het menu dat volgt ‘GVB ‘Desktop’’. Medewerker zit nu in de eigen GVB omgeving.
    i) De uitgebreide handleiding is te vinden in

ii) Bijlage 1.

4 Datalekken

4.1 Werken met persoonsgegevens

Medewerkers die werken met persoonsgegevens, zoals klantgegevens, camerabeelden en reisgegevens moeten ervoor zorgen dat deze informatie binnen de digitale muren van GVB blijft.

4.2 Melden van vermoeden van datalek

De medewerker die vermoedt dat persoonsgegevens (mogelijk) op werk, thuis of elders zijn kwijtgeraakt, meldt dit onmiddellijk bij meldpuntdatalek@gvb.nl. Dit is een niet-uitputtende lijst met voorbeelden van datalekken:

a. De werktelefoon, laptop of Ipad waarop persoonsgegevens staan van bijvoorbeeld reizigers of medewerkers, is gestolen of kwijtgeraakt;
b. Het ter beschikking stellen van privé apparatuur met persoonsgegevens van GVB aan derden, zoals bij weggooien, inruilen, weggeven of verkopen;
c. Medewerker stuurt een e-mail met persoonsgegevens aan de verkeerde persoon;
d. Een inbraak door een hacker;
e. Medewerker heeft zonder toestemming inzicht gehad in persoonsgegevens, bijvoorbeeld door een onjuiste autorisatie/toegang tot een database.

4.3 Privacyregels

Ter voorkoming van datalekken houdt de medewerker zich aan de volgende privacyregels:

- Wachtwoorden zijn strikt persoonlijk. Geef deze nooit aan collega's of aan anderen, en bewaar ze op een veilige plek.
- Wees voorzichtig met het openen van mails, zeker van onbekende personen. Open nooit een verdachte e-mail (en/of bijlage), maar meld deze bij de ICT-helpdesk en gooi hem direct weg Servicedesk ICT.
- Stuur nooit GVB mails naar een privéadres (bijv. ikwerkbijGVB@hotmail.com).
- Bedenk van tevoren welke informatie je wel en niet mag delen met derden, zoals met familie en vrienden, op social media of aan de telefoon. Of als je zaken doet met een bedrijf dat werk voor ons uitvoert.
- Print geen documenten met persoonsgegevens of bedrijfsinformatie. Mocht je toch moeten printen, verscheur dan de prints als je ze niet meer nodig hebt en bewaar ze om bij GVB weg te gooien in de gele papierbak. Je kunt de prints ook volledig versnipperen, zodat ze niet meer leesbaar zijn. In dat geval kun je ze thuis weggooien.
- Je werkt met persoonsgegevens van collega's en reizigers en met bedrijfsgegevens. **Houd de regels van vertrouwelijkheid of geheimhouding in acht**.
- **Vergrendel altijd je computer**, ook als je maar even weggaat.
- **Gebruik persoonsgegevens alleen voor het doel waarvoor GVB ze heeft verzameld.**
- **Bewaar persoonsgegevens niet langer dan nodig.** Als je ze niet meer nodig hebt, gooi ze dan weg, ook uit bijvoorbeeld de persoonlijke mappen van je mailbox en op netwerkschijven.
- Weet dat je met vragen over privacy terecht kunt bij het GVB Privacy Team, bereikbaar via: privacy@gvb.nl.
- Per ongeluk persoonlijke of vertrouwelijke informatie gedeeld? Je telefoon, iPad of laptop kwijtgeraakt? Of anders? Meld het bij meldpuntdatalek@gvb.nl, zodat we het probleem direct kunnen oplossen.

4.4 Op afstand wissen van gegevens

Zakelijke gegevens op devices (mobiele apparaten) kunnen worden gewist zodra er sprake is van verlies of diefstal. Op afstand wissen is niet mogelijk voor devices (mobiele apparaten) die voor 1 juni 2020 zijn uitgegeven.

5 Beheerders

5.1 Vertrouwelijkheid

Beheerders hebben een bijzondere positie, omdat zij in principe alle informatie en handelingen van medewerkers van GVB kunnen inzien. Beheerders moeten persoonsgegevens die zij door hun activiteiten als beheerder te weten komen, strikt vertrouwelijk behandelen. Vanwege deze bijzondere positie weegt schending van deze plicht zwaar.

5.2 Toegang tot accounts of computers van medewerkers

In overeenstemming met het Protocol voor integriteitonderzoeken (zoals bedoeld in artikel 15.16 cao GVB) geven beheerders zich slechts toegang tot accounts of computers van medewerkers, als daarvoor opdracht is gegeven door de directie.

5.3 Taken en bevoegdheden van beheerders

a. Beheerders moeten activiteiten die inzage in persoonsgegevens van individuele medewerkers kunnen opleveren beperken tot het uiterste. Daarbij geeft GVB beheerders geen opdrachten of dienstbevelen die in strijd zijn met het ICT Protocol.
b. De beheerders moeten altijd in overeenstemming met het ICT Protocol en de relevante wet- en regelgeving handelen. Hieronder valt onder andere de Algemene Verordening Gegevensbescherming.
c. In geval van een datalek meldt de Beheerder dit bij de Functionaris Gegevensbescherming. De Functionaris Gegevensbescherming beoordeelt of een melding bij de Autoriteit Persoonsgegevens en bij belanghebbenden moet worden gemaakt.

6 Monitoring en controle

6.1 Registratie van ICT-middelen

GVB legt het gebruik van ICT-middelen vast door loggen (geautomatiseerde verzameling).

6.2 Controle op het gebruik ICT-middelen

De controle op het gebruik van door GVB ter beschikking gestelde ICT-middelen gebeurt alleen als de medewerker een van de genoemde richtlijnen (artikel 2.3) overtreedt. De controle valt onder de verantwoordelijkheid van de directeur ICT&Innovatie. GVB hanteert daarbij de volgende aanpak:

a. Voor het tegengaan van virussen en andere schadelijke programma's, in het kader van systeem- en netwerkbeveiliging, wordt het e-mail- en internetgebruik op geautomatiseerde wijze gecontroleerd;
b. Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot geanonimiseerde verkeersgegevens (onder andere: tijd, hoeveelheid en omvang)

Daarnaast kunnen in opdracht van de compliance officer kunnen de volgende controles worden uitgevoerd:

c. Controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek;

d. Controle in het kader van het tegengaan van overlastgevend gebruik vindt plaats na een concrete klacht of in het kader van een algemeen, niet op individuen gericht onderzoek, waarbij het Protocol voor integriteitonderzoeken van toepassing is;

Er wordt een verslag opgesteld van een controle (wanneer, door wie, eventueel over wie en waarom een controle heeft plaatsgevonden). Als de controle - in tweede instantie - gericht is geweest op een of meerdere medewerker(s), dan zal het verslag met de medewerker(s) worden gedeeld en worden aangeleverd aan de compliance officer die het zal archiveren.

6.3 Inhoudelijke controle ICT-middelen

Inhoudelijke controle van door GVB ter beschikking gestelde ICT-middelen gebeurt alleen als er op basis van concrete aanwijzingen een vermoeden van integriteitschending is ontstaan zoals bedoeld in het Protocol voor integriteitonderzoeken.

6.4 Integriteitsonderzoek

Een onderzoek naar aanleiding van een vermoeden van integriteitschending door oneigenlijk gebruik van digitale communicatiemiddelen vindt in principe in stappen plaats. Er zijn verschillende onderzoek stappen. Het besluit om over te gaan naar de volgende onderzoek stap gebeurt na een zorgvuldige belangenafweging over het recht op privacy van de persoon in kwestie en het belang van het onderzoek. Lees het Protocol voor integriteitsonderzoeken (paragraaf 4.7) voor meer informatie over dit onderzoek.

6.5 AVG en andere wet- en regelgeving

GVB zal bij de controle altijd de Algemene Verordening Gegevensbescherming (AVG) en andere relevante wet- en regelgeving naleven.

6.6 Afwijking van regeling

De controle op door GVB ter beschikking gestelde ICT-middelen binnen GVB wordt alleen volgens deze regeling uitgevoerd. Alleen zwaarwegende en onvoorziene omstandigheden kunnen vereisen dat hiervan wordt afgeweken. GVB zal in dat geval zo snel mogelijk toelichten waarom dat is gebeurd. Als zulke situaties zich voordoen, dan beslist de algemeen directeur, met inachtneming van de relevante wet- en regelgeving en na overleg met de ondernemingsraad, of hiervan afgeweken wordt.

6.7 Controle door beheerder

Beheerder voert de controle op ICT-middelen van een medewerker uit, nadat de directie opdracht tot uitvoering heeft gegeven. De beheerder neemt hierbij de regels van hoofdstuk 5 van dit protocol in acht. Beheerder rapporteert aan de directie. De betreffende medewerker en diens leidinggevende ontvangen hiervan mededeling.

6.8 Specifieke gegevens over het gebruik van ICT-middelen

Gegevens over het gebruik van ICT-middelen door een specifieke medewerker zijn persoonsgegevens en worden daarom niet langer bewaard dan noodzakelijk, met een maximum termijn van twee jaar.

7 Sancties

7.1 In gesprek

Medewerkers die zich niet aan dit ICT Protocol houden, worden zo snel mogelijk door de leidinggevende op hun gedrag aangesproken. Dit kan leiden tot een onderzoek in de zin van het Protocol integriteitsonderzoeken.

7.2 Disciplinaire maatregelen

Bij handelen in strijd met dit ICT Protocol of de algemeen geldende wettelijke regels, kan GVB afhankelijk van de aard en de ernst van de overtreding disciplinaire maatregelen treffen. Hieronder valt een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst of het inhuurcontract. Bij constatering van strafbare feiten kan GVB daar aangifte van doen.

8 Regeling bij einde samenwerking met medewerker

8.1 Einde arbeids- of inhuurovereenkomst

Dit artikel is van toepassing als de samenwerking tussen medewerker en GVB eindigt.

8.2 Inleveren ICT-middelen

Bij beëindiging van de samenwerking geeft de medewerker alle door GVB ter beschikking gestelde ICT-middelen terug aan de beheerder op de laatste dag van de samenwerking. De leidinggevende van de medewerker zorgt voor een tijdige en zorgvuldige overdracht van de shares en bestanden binnen de afdeling in het belang van de continuïteit van de bedrijfsvoering. De medewerker stelt zelf eventuele privégegevens die op de ICT-middelen staan veilig.

8.3 Digitale bestanden en software

In overleg met de leidinggevende draagt de medewerker alle bestanden en software die de medewerker op eigen (niet door GVB ter beschikking gestelde) ICT-middelen heeft ingezet over aan de Beheerder. Na afronding van de data-overdracht vernietigt de medewerker deze.

9 Overige bepalingen

9.1 Jaarlijkse evaluatie

Dit ICT Protocol wordt jaarlijks geëvalueerd door GVB. De uitkomst van de evaluatie wordt altijd besproken met de OR.

GVB kan dit ICT Protocol na instemming van de OR wijzigen als de evaluatie, omstandigheden of verandering in wetgeving daar aanleiding toe geven. Deze wijzigingen worden aan medewerkers bekend gemaakt.

10 Gebruikersovereenkomst

10.1 Gebruikersovereenkomst voor inhuurmedewerkers

De gebruikersovereenkomst maakt onderdeel uit van dit protocol. Door GVB ingehuurde medewerkers dienen de gebruikersovereenkomst te ondertekenen. Deze wordt opgeborgen door de leidinggevende.

11 Bijlage 1

(terug naar 3.2)

11.1 De digitale werkplekALW

Benaderen via een eigen device (thuis en op kantoor).
In deze handleiding is gebruik gemaakt van diverse devices. Schermen kunnen (per device) afwijken.

11.2 Eerste keer inloggen

Ga in je browser naar http://ci.gvb.nl en log in met je GVB gegevens. Om de omgeving te gebruiken moet je eenmalig een Citrix Workspace installeren.

11.3 Citrix Workspace

Afhankelijk van je device krijg je de eerste keer het verzoek om een Citrix Workspace te installeren. Krijg je de vraag niet en heb je nog geen Citrix Workspace geïnstalleerd op je device? Kijk dan voor de juiste versie op: https://www.citrix.com/nl-nl/products/receiver.html. Download en installeer de Citrix Workspace voor jouw device. De applicatie verzorgt straks de verbinding met jouw werkplek.

Vanuit Citrix worden momenteel elk device ondersteund, inclusief smartphones, tablets, pc's en Macs.

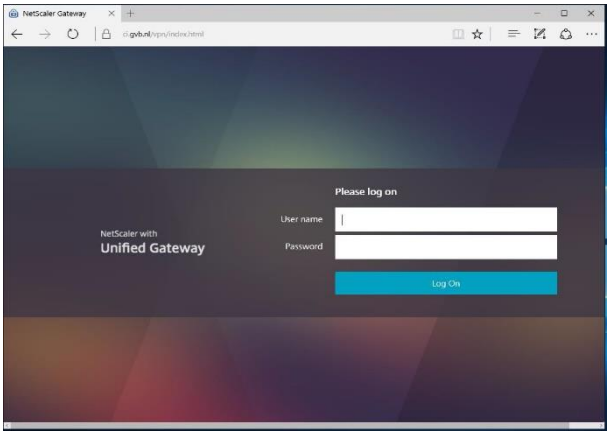
11.4 Installeren

Installeer de applicatie. Ga akkoord met de Citrix licentie en klik op 'installeren'. Volg de menu-opties en geef Citrix toegang waar nodig.

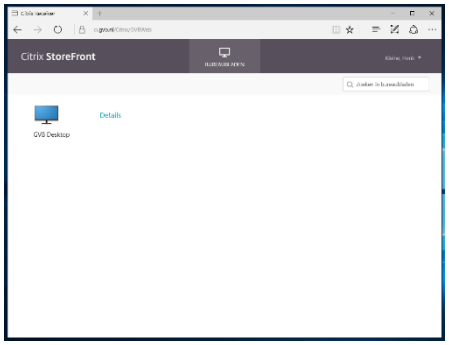
Krijg je vragen over Single sign on en delen van anonieme gegevens? Selecteer deze niet. Je kunt dit eventueel later altijd nog aanpassen in de instellingen.
Android vraagt je tijdens de installatie specifiek om account gegevens, je hoeft hier niets in te vullen, je bent klaar met het installeren van de applicatie.

11.5 Inloggen op de digitale werkomgeving

(Via de link: https://ci.gvb.nl en Citrix Workspace geïnstalleerd)
Log in met je GVB gebruikersnaam en wachtwoord.



Je komt nu in de ‘Citrx StoreFront’. Selecteer de GVB desktop.



11.6 .ica bestand openen

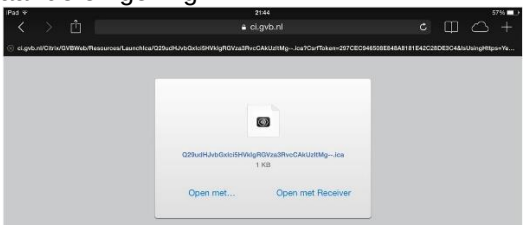
Open na het aanklikken het ICA bestand dat wordt aangeboden. Op sommige devices gaat dit vanzelf, op andere devices moet je het bestand specifiek openen.

Voorbeeld Windows

Selecteer openen, de Citrix Workspace opent met de instellingen uit file en gaat naar de omgeving.

Voorbeeld IOS

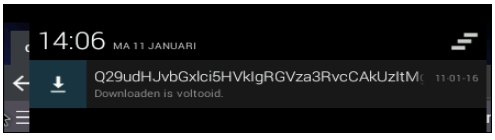
Selecteer Openen met Workspace, de Citrix Workspace opent met de instellingen uit file en gaat naar de omgeving.



Voorbeeld Android

Ga naar downloads

Kijk bij het download icoon. Hier staat een xxxxxxxx.ica file (met veel random letters/cijfers) . Klik deze aan. De Citrix Workspace opent met de instellingen uit file en gaat naar de omgeving.



Na het accepteren van de ICA file en het openen met Workspace kom je in de Digitale werkomgeving ALW.