

Inhoud

1. Definities.....	3
2. Algemene uitgangspunten:	4
3. Bepalingen omtrent door GVB ter beschikking gestelde ICT-Middelen en ICT-Diensten	5
4. Bijzondere bepalingen over sociale media	6
5. Melden Datalekken	7
6. Bijzondere bepalingen voor Beheerders.....	7
7. Monitoring en controle.....	7
8. Sancties.....	9
9. Rechten van Medewerkers	9
10. Exit-regeling	9
11. Overige bepalingen	10
12. Gebruikersovereenkomst.....	10
Bijlage Specifieke gebruikersbepalingen, wachtwoorden en gegevensdragers.....	11
Gebruikersovereenkomst behorende bij het ICT-Protocol.....	13

Datum: 12 september 2017

In dit ICT-Protocol worden regels gesteld voor het gebruik van door GVB ter beschikking gestelde ICT-Middelen en ICT-Diensten door Medewerkers van GVB. Ook de manier waarop controle en toezicht plaatsvindt wordt in dit ICT-Protocol omschreven. Dit ICT-Protocol geldt voor alle Medewerkers van GVB.

1. Definities

- 1.1 Medewerker: Iedere persoon in dienst van GVB, alsmede personen die door GVB worden ingehuurd om werkzaamheden voor GVB te verrichten.
- 1.2 ICT-Middelen: hardware, software en netwerkfaciliteiten, waaronder – maar niet uitsluitend – internet, e-mail, telefoon, computer- en randapparatuur in de ruimste zin des woords.
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 (BYOD – Bring Your Own Device).
- 1.3 Bring Your Own Device (BYOD): is een beleid waarin medewerkers, zakelijke partners en andere gebruikers in staat worden gesteld om persoonlijk geselecteerde en gekochte client (computer) apparatuur - zoals smartphones, tablets en laptops – thuis, onderweg of op de werkplek te gebruiken en met het GVB bedrijfsnetwerk te verbinden.
- 1.4 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 ter beschikking gestelde doeleinden gebruikt worden.
- 1.5 Bedrijfsgegevens: alle gegevens waarvoor GVB verantwoordelijk is en op aangesproken kan worden indien daar onrechtmatig mee wordt omgegaan.
- 1.6 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.
- 1.7 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.
- 1.8 Datalek: Bij een datalek gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij GVB zonder dat dit de bedoeling is.
- 1.9 Privacy Officer: Degene die namens GVB verantwoordelijk is voor het volledige overzicht van persoonsgegevens waarvoor GVB verantwoordelijk is, die in ICT-Diensten en ICT-Middelen vastgelegd zijn en hij is ook degene die op de hoogte gesteld moet worden als persoonsgegevens ongeautoriseerd buiten GVB zijn beland.

- 1.10 Voor GVB medewerkers wordt het ICT Protocol getekend bij indiensttreding en is daardoor onderdeel van de arbeidsovereenkomst. Voor zittende GVB medewerkers is het ICT-Protocol (zoals vastgesteld op 12 september 2017) van toepassing door opname van een bepaling in de cao (artikel 14.18). De cao wordt in de arbeidsovereenkomst van toepassing verklaard op de medewerker.
- Voor personen die door GVB worden ingehuurd wordt het ICT Protocol getekend bij aanvaarding van de opdracht en is daardoor onderdeel van de inhuurovereenkomst.. Het ICT Protocol is tot stand gekomen met instemming van de OR.
- 1.11 Sociale media is een verzamelbegrip voor online platformen waar de gebruikers, zonder of met minimale tussenkomst van een professionele redactie, de inhoud verzorgen. Hoofdkenmerken zijn interactie en dialoog tussen de gebruikers. Via deze media delen mensen verhalen, kennis en ervaringen.

2. Algemene uitgangspunten:

- 2.1 Gebruik van ICT-Middelen en ICT-Diensten is voor velen binnen GVB nodig om de werkzaamheden gedegen uit te voeren. Onjuiste omgang met ICT-middelen dan wel misbruik kost tijd en capaciteit van mensen en apparatuur en brengt diverse risico's met zich mee. Bovendien bestaat het risico op het in strijd handelen met wet- en regelgeving en op beveiligingsincidenten, waaronder datalekken.
- 2.2 Tegen de achtergrond van de risico's van het gebruik van ICT-middelen, wordt van de Medewerker professioneel, integer en zorgvuldig handelen verwacht.
- 2.3 GVB bedrijfsgegevens zijn toegankelijk met ICT-Middelen en ICT-Diensten die door GVB ter beschikking zijn gesteld. GVB staat het gebruik door Medewerkers van niet door GVB ter beschikking gestelde ICT-Middelen voor zakelijk gebruik toe, mits er geen bedrijfsgegevens op die privé-middelen worden opgeslagen.
- De niet door GVB ter beschikking gestelde ICT-Middelen worden niet door GVB onderhouden. Medewerker zorgt er zelf voor dat het ICT-Middel waar hij mee werkt veilig is.
- 2.4 Alle Bedrijfsgegevens blijven binnen de ICT-Middelen en ICT-Diensten van GVB en niet daarbuiten, zoals op de ICT-Middelen en ICT-Diensten van Medewerker.
- In het kader van hun taakuitoefening kunnen GVB medewerkers GVB-bedrijfsgegevens uitwisselen met zakelijke partners van GVB, tenzij deze gegevens persoonsgegevens bevatten. In het laatste geval kan het uitsluitend als daarvoor afspraken worden gemaakt met de ontvangende partij bijvoorbeeld inzake het gebruik van de gegevens, de beveiliging, de vernietiging na gebruik en eventueel geval van een datalek. Mogelijk is een verwerkersovereenkomst noodzakelijk. Omdat de feitelijke omstandigheden bepalend zijn, is de beoordeling maatwerk en dient contact te worden opgenomen met de privacy officer.
- 2.5 Met persoonlijk toegekende inloggegevens en eventuele aanvullende authenticatiemiddelen (zoals smartcards en tokens) en overige beveiligingshulpmiddelen dient zorgvuldig te worden omgegaan. Persoonsgebonden wachtwoorden en aanvullende authenticatiemiddelen mogen niet worden gedeeld.

- 2.6 Privégebruik van ICT-Middelen onder werktijd is incidenteel toegestaan, mits dit gebruik in overeenstemming is met dit ICT-Protocol en in geen geval storend is voor, dan wel ten koste gaat van, het uitvoeren van de dagelijkse werkzaamheden.

3. Bepalingen omtrent door GVB ter beschikking gestelde ICT-Middelen en ICT-Diensten

- 3.1 GVB behoudt zich het recht voor om de toegang tot niet-functionele sites of de toegang tot bepaalde telefoonnummers te beperken. Met name sites of telefoonnummers waarvoor betaald moet worden, of met een pornografische, racistische, discriminerende, op entertainment, geweld of op commercie gerichte inhoud zullen worden geweerd.
- 3.2 De regels die momenteel gelden voor het ondertekenen van schriftelijke correspondenties, correct taalgebruik, het vertegenwoordigen van GVB en voor het verzenden van post zijn ook van toepassing op e-mail en dergelijke.
- 3.3 Het is niet toegestaan om illegale of ongewenste content te downloaden, waaronder wordt verstaan:
- a. sites te bezoeken die pornografische, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten; noch is het toegestaan dergelijk materiaal te downloaden;
 - b. zich ongeoorloofd toegang te verschaffen tot niet openbare bronnen op het internet (hacken);
 - c. informatie waartoe men via internet toegang heeft verkregen opzettelijk en zonder toestemming te veranderen of te vernietigen (vorm van hacken);
 - d. filescharen buiten de GVB omgeving;
 - e. gebruik maken van streamingdiensten (zoals internetradio of Uitzending gemist), tenzij dit voor het werk noodzakelijk is;
 - f. films, muziek, applicaties en overig auteursrechtelijk beschermd materiaal te downloaden van een evident illegale bron;
 - g. het versturen van berichten aan een groot aantal ontvangers, kettingbrieven en kwaadaardige software zoals virussen, spyware of Trojaanse paarden;
- Bij email is het is niet toegestaan om:
- h. berichten anoniem of onder een fictieve naam te versturen;
 - i. dreigende, beledigende, aanstootgevende, seksueel getinte, racistische, discriminerende berichten of kettingmailberichten te verzenden of door te sturen;
 - j. iemand elektronisch lastig te vallen;
 - k. Met betrekking tot intern e-mail gebruik geldt de regel dat de adressering "alle gebruikers/ Medewerker" uitsluitend met toestemming van de bevoegd leidinggevende wordt gebruikt.
 - l. bewust virussen, Trojaanse paarden, spyware en dergelijke te versturen.

Indien Medewerker ongevraagd informatie van deze aard aangeboden krijgt, dient Medewerker dit aan de leidinggevende te melden.

- 3.4 Bij twijfel over de in 3.3 genoemde regels kan je contact opnemen met je leidinggevende. Mocht dat gezien de situatie niet wenselijk zijn, dan kan je contact opnemen met het Meldpunt Integriteit. In de cao is een gedragslijn vermoeden van misstanden opgenomen.

- 3.5 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.
- 3.6 Indien medewerker zelf niet in staat is om zich toegang te verschaffen tot door GVB ter beschikking gestelde ICT-Middelen, is GVB gerechtigd beheerder op verzoek van de leidinggevende daartoe toegang te verschaffen, indien er sprake is van een zwaarwegend bedrijfsbelang.
De beheerder mag zich echter geen toegang verschaffen tot niet-door-GVB-ter-beschikking-gestelde gemarkeerde mappen, bestanden, of (mail)folders. GVB zal door inschakeling van een vertrouwenspersoon de computer van Medewerker controleren om zo privémails en -bestanden te herkennen en in een aparte map te plaatsen alvorens Beheerder toegang krijgt.
Van de actie wordt een verslag opgesteld van wanneer, door wie, over wie en waarom de actie heeft plaatsgevonden. Het verslag, dat met de medewerker wordt gedeeld, wordt aangeleverd aan de privacy officer die het zal archiveren.

4. Bijzondere bepalingen over sociale media

- 4.1 GVB ondersteunt de open dialoog en de uitwisseling van ideeën en het delen van kennis via sociale media zoals blogs, forums, LinkedIn, wiki's of Twitter. Indien dit werkgerelateerde onderwerpen betreft, dient Medewerker ervoor te zorgen dat het profiel en de inhoud in overeenstemming is met hoe hij zich in tekst, beeld en geluid zou presenteren ten overstaan van collega's en klanten.
Medewerkers mogen geen persoonsgegevens, vertrouwelijke en/of schadelijke informatie verstrekken over GVB, klanten, partners of leveranciers zonder hun goedkeuring.
Plaats geen berichten die het imago van GVB kunnen schaden.
- 4.2 Verder dient Medewerker bij werkgerelateerde onderwerpen altijd GVB en zijn functie te vermelden, alsmede een disclaimer waarin staat dat het een persoonlijk standpunt betreft, dat niet overeen hoeft te komen met dat van de organisatie. Desondanks blijft het de plicht van Medewerker om zich fatsoenlijk te gedragen.
- 4.3 Medewerker is geen woordvoerder van GVB en je spreekt dus niet namens GVB.
Medewerker dient terughoudend te zijn met uitspraken over (producten van) concurrenten, aangezien dit kan worden opgevat als vergelijkende reclame of oneerlijke handelspraktijken van GVB en daarmee tot boetes voor het bedrijf kan leiden. In ieder geval is het om deze reden Medewerker verboden een mening over GVB of concurrenten te geven zonder zich als Medewerker van GVB kenbaar te maken.
- 4.4 Bestuurders, managers, leidinggevend en degene die namens de organisatie het beleid en de strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruik van sociale media, ook als de inhoud niet direct verband houdt met hun werk. Op grond van hun positie moeten zij nagaan of zij op persoonlijke titel kunnen publiceren. Zij zijn zich ervan bewust dat Medewerkers lezen wat zij schrijven.
- 4.5 Dit artikel 4 (Bijzondere bepalingen over sociale media) geldt ook indien Medewerkers vanaf privé-accounts deelnemen aan sociale media.

5. Melden Datalekken

- 5.1 Medewerkers die werken met privacy gevoelige informatie, zoals klantgegevens, camerabeelden en OV-Chipkaartgegevens moeten ervoor zorgen dat deze informatie binnen de digitale muren van GVB blijft.
- 5.2 De Medewerker die vermoedt dat hij op werk, thuis, of elders privacy gevoelige informatie (mogelijk kwijt is geraakt, meldt dit onmiddellijk bij meldpuntdatalek@gvb.nl. In het geval van een datalek moet GVB dit onmiddellijk melden bij de overheid - Autoriteit Persoonsgegevens. Als dit niet of te laat gebeurt, loopt GVB het risico van een enorm hoge boete.
- Voorbeelden van datalekken zijn:
- a. Het ter beschikking stellen van privé apparatuur met persoonsgegevens van GVB aan derden, zoals bij weggooien, inruilen, weggeven of verkopen;
 - b. een gestolen of verloren laptop, telefoon, I-pad of USB stick;
 - c. een inbraak door een hacker;
 - d. (per ongeluk) ongeautoriseerd verstrekken van Persoonsgegevens aan derden;
 - e. menselijk falen (zoals te eenvoudige wachtwoorden, het verstrekken van username/wachtwoord aan collega's en externen);
 - f. een malware-besmetting.

6. Bijzondere bepalingen voor Beheerders

- 6.1 Omdat Beheerders in beginsel alle informatie en handelingen van Medewerkers van GVB kunnen inzien, hebben zij een bijzondere positie. Beheerders dienen privacygevoelige informatie en persoonsgegevens die zij in het kader van hun activiteiten als Beheerder te weten komen, strikt vertrouwelijk te behandelen. Schending van deze plicht weegt zwaar gezien hun bijzondere positie.
- 6.2 Beheerders dienen activiteiten die inzage in privacy gevoelige informatie of persoonsgegevens van individuele medewerkers kunnen opleveren, tot het uiterste te beperken, behoudens het in dit ICT-Protocol gestelde.
- 6.3 In overeenstemming met het protocol voor integriteitsonderzoeken zoals bedoeld in artikel 14.17 van de cao verschaffen Beheerders zich slechts toegang tot accounts of computers van Medewerkers, indien daarvoor opdracht is gegeven door directie.
- 6.4 GVB zal Beheerders geen opdrachten of dienstbevelen geven ten aanzien van privacygevoelige informatie en persoonsgegevens die in strijd zijn met dit ICT Protocol.
- 6.5 Beheerders dienen te allen tijde in overeenstemming met dit ICT-Protocol en de relevante wet- en regelgeving, waaronder – maar niet uitsluitend – de Wet bescherming persoonsgegevens te handelen. In geval van een datalek zal de Beheerder dit melden bij de Privacy Officer. De Privacy Officer meldt het overeenkomstig de relevante wet- en regelgeving bij de Autoriteit Persoonsgegevens en bij belanghebbenden.

7. Monitoring en controle

- 7.1 De controle op door GVB ter beschikking gestelde ICT-middelen binnen GVB zal alleen conform deze regeling worden uitgevoerd, tenzij zwaarwegende en onvoorziene omstandigheden vereisen dat hiervan afgeweken wordt. GVB zal in dat geval zo snel als mogelijk toelichten waarom dat is gebeurd. Indien zulke situaties zich voordoen, beslist de

algemeen directeur, met inachtneming van de relevante wet- en regelgeving, en na overleg met de ondernemingsraad.

- 7.2 Het gebruik van ICT-middelen wordt vastgelegd. Dit gebeurt door middel van geautomatiseerde verzameling (loggen).
- 7.3 De controle op door GVB ter beschikking gestelde ICT-middelen vindt slechts plaats in het kader van de in artikel 3.3 genoemde richtlijnen. Daarbij hanteert GVB de volgende aanpak:
- 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;
 - Controle op het uitlekken van bedrijfsgeheimen vindt plaats op basis van steekproefsgewijze contentfiltering. Een verdacht bericht wordt apart gezet voor nader onderzoek;
 - 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 gestelde in het Protocol voor integriteitonderzoeken van toepassing is.;
 - Controle in het kader van kosten- en capaciteitsbeheersing wordt beperkt tot geanonimiseerde verkeersgegevens (tijd, hoeveelheid, omvang, ed.)
 - Van een controle wordt een verslag opgesteld van wanneer, door wie, eventueel over wie en waarom een controle heeft plaatsgevonden. Indien de controle - in tweede instantie - gericht is geweest op een of meerdere medewerker(s), dan zal het verslag, dat met de medewerker(s) wordt gedeeld, worden aangeleverd aan de compliance officer die het zal archiveren.
- 7.4 Inhoudelijke controle van door GVB ter beschikking gestelde ICT-middelen zal slechts plaatsvinden indien er op basis van concrete aanwijzingen een vermoeden van een integriteitschending is ontstaan zoals bedoeld in het Protocol voor integriteitonderzoeken.
- 7.5 GVB zal bij de controle te allen tijde de Wet bescherming persoonsgegevens (Wbp) en andere relevante wet- en regelgeving naleven. In het bijzonder zal GVB de bij controle vastgelegde gegevens beveiligen tegen ongeautoriseerde toegang en zijn Beheerders die toegang hebben tot de gegevens verplicht tot geheimhouding.
- 7.6 Gegevens over het gebruik van ICT-middelen zijn persoonsgegevens en generiek worden ze daarom niet langer bewaard dan noodzakelijk, met een maximum termijn van een jaar.
- 7.7 Ten behoeve van de beschikbaarheid van de infrastructuur en diensten worden met een zekere regelmaat de niet voor zakelijk gebruik bestemde bestanden van het netwerk verwijderd.
- 7.8 De controle wordt uitgevoerd door Beheerder, nadat de directie opdracht tot uitvoering heeft gegeven en met in achtneming van hetgeen overigens in dit ICT-Protocol staat verwoord. Beheerder rapporteert aan de directie. De betreffende Medewerker en diens leidinggevende ontvangen hiervan mededeling.
- 7.9 E-mailberichten in het kader van de werkzaamheden van leden, voormalige en kandidaat-leden van de medezeggenschapsorganen, vakbondskaderleden, van bedrijfsartsen, vertrouwenspersonen en een ieder die zich op grond van zijn functie op enige vertrouwelijkheid

moet kunnen beroepen, worden niet inhoudelijk gecontroleerd. Na toestemming van betrokkenen mag controle op de veiligheid van berichtenverkeer plaatsvinden.

8. Sancties

- 8.1 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 vallen een waarschuwing, berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst of het inhuurcontract. Bij constatering van strafbare feiten is GVB voornemens daarvan aangifte te doen.
- 8.2 Medewerkers ten aanzien van wie geconstateerd is dat zij zich niet aan dit ICT-Protocol houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken. Mogelijk kan dit leiden tot een integriteitsonderzoek. Volgens het Protocol voor integriteitsonderzoeken krijgen zij daarbij inzage in de over hen vastgelegde gegevens en hebben de gelegenheid te reageren op het geconstateerde. Medewerker en leidinggevende maken dan afspraken voor de toekomst en de leidinggevende bepaalt de mogelijke sanctie(s) bij overtreding daarvan. Deze afspraken kunnen strenger zijn dan het in dit ICT-Protocol bepaalde. Ook kan de toegang tot ICT-middelen worden beperkt of geheel worden afgesloten. Het gebruik van niet door GVB ter beschikking gestelde ICT-Middelen voor door GVB ter beschikking gestelde doeleinden kan door GVB worden beperkt.

9. Rechten van Medewerkers

- 9.1 Medewerker kan zich tot zijn leidinggevende wenden met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens onder deze gedragscode. Het verzoek wordt binnen vier weken beantwoord.
- 9.2 Medewerker kan GVB verzoeken de verwerkte persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor de doelen van deze gedragscode onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift. Het verzoek wordt binnen vier weken beantwoord.
- 9.3 Medewerker kan verder verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met zwaarwegende persoonlijke omstandigheden. GVB oordeelt binnen vier weken na ontvangst van het verzet of dit gerechtvaardigd is. Indien GVB het verzet gerechtvaardigd acht, beëindigt zij terstond de verwerking.

10. Exit-regeling

- 10.1 Indien de samenwerking tussen Medewerker en GVB eindigt is dit artikel van toepassing. Onder einde van de samenwerking valt onder andere – maar niet uitsluitend - het einde van het dienstverband en het einde van de inhuurovereenkomst.
- 10.2 Alle zakelijk beschikbaar gestelde ICT-middelen, alsmede alle door GVB ter beschikking gestelde gegevens blijven te allen tijde eigendom van GVB.
- 10.3 Bij beëindiging van de samenwerking zal Medewerker alle door GVB ter beschikking gestelde ICT-middelen onmiddellijk afgeven aan Beheerder. De leidinggevende van de Medewerker draagt zorg voor een tijdige en zorgvuldige overdracht van de shares en bestanden binnen de

afdeling in het belang van de continuïteit van de bedrijfsvoering. Medewerker is zelf verantwoordelijk voor het veiligstellen van alle privégegevens die op de ICT-middelen staan.

- 10.4 Voor niet door GVB ter beschikking gestelde ICT-Middelen die voor zakelijk gebruik zijn ingezet, geldt dat Medewerker alle door GVB ter beschikking gestelde bestanden en software moet overdragen aan Beheerder. Na afronding van de data-overdracht dienen alle door GVB ter beschikking gestelde bestanden en software te worden vernietigd.

11. Overige bepalingen

- 11.1 Deze regeling wordt jaarlijks geëvalueerd door GVB. De evaluatie wordt altijd besproken met de OR. Deze regeling kan worden aangepast na instemming van de OR. Medewerker dan wel Beheerder wordt hierover door GVB geïnformeerd.
- 11.2 GVB kan dit ICT-Protocol na instemming van de OR wijzigen als de omstandigheden dan wel verandering in wetgeving daar aanleiding toe geven. Deze wijzigingen worden voorafgaand aan de invoering aan Medewerkers bekend gemaakt.

12. Gebruikersovereenkomst

De gebruikersovereenkomst, welke onderdeel uitmaakt van dit protocol, zal aan eenieder die voor GVB werkzaam is ter ondertekening worden aangeboden.

Van medewerkers die in dienst zijn van GVB wordt de ondertekende gebruikersovereenkomst in het personeelsdossier opgeborgen.

Van door GVB ingehuurd medewerkers wordt de ondertekende gebruikersovereenkomst opgeborgen door de leidinggevende waarvoor hij of zij werkt.

Bijlage Specifieke gebruikersbepalingen, wachtwoorden en gegevensdragers

- 1 De virtuele desktop van GVB (Citrix) is de standaard oplossing om met behulp van ICT-Middelen en ICT-Diensten toegang te hebben tot GVB bedrijfsgegevens. Dit geldt voor de werkplek thuis, onderweg en op GVB locaties.
- 2 Medewerker dient wachtwoorden van GVB te allen tijde strikt geheim te houden en regelmatig te wijzigen.
GVB gebruikt de instellingen van Microsoft sterke wachtwoorden policy.
Overige wachtwoorden dienen minimaal uit 8 tekens te zijn, dienen diverse karakters te bevatten (minimaal 1 hoofdletter, minimaal 1 kleine letter en 1 cijfer) en dienen uiteraard niet voor de hand te liggen (bijvoorbeeld de naam met geboortjaar erachter). Indien het wachtwoord is gelekt dient Medewerker dit onverwijld aan GVB ICT Service Desk te melden.
In geval van ontvangen gegevensdragers – waaronder ook prints - dient Medewerker na gebruik zorgvuldig om te gaan met de bewaring en afvoer, vernietiging of inlevering ervan.
- 3 Voor bestandsuitwisseling wordt gebruik gemaakt van GVB door GVB ter beschikking gestelde tools, zoals SFTP; OneDrive for Business, of de GVB Sharepoint omgeving.
Medewerker mag alleen gegevensdragers, waaronder USB-sticks, inzetten indien de gegevens op deze dragers geëncrypt en voorzien van een sterk wachtwoord zijn.
In geval van ontvangen gegevensdragers – waaronder ook prints - dient Medewerker na gebruik zorgvuldig om te gaan met de bewaring en afvoer, vernietiging of inlevering.
- 4 Gezien de veiligheidsaspecten gelden de volgende uitgangspunten voor het gebruik van ICT-middelen en ICT-Diensten in de algemene zin:
 - a. Voor werkzaamheden die onder een bepaalde inlognaam worden uitgevoerd draagt de betreffende Medewerker de verantwoordelijkheid.
 - b. Medewerkers die door GVB worden ingehuurd om werkzaamheden voor GVB te verrichten, worden uitsluitend in staat gesteld om op GVB netwerk te werken na toestemming van de hiertoe bevoegde GVB Medewerker.
 - c. Medewerkers zorgen ervoor dat alvorens de werkplek wordt verlaten systemen worden vergrendeld (windows tekentje, L) en door middel van een vergrendeling als de screensaver verschijnt (maximaal 5 minuten).
 - d. Vertrouwelijke gegevens en bedrijfsgevoelige informatie mogen uitsluitend met toestemming van de leidinggevende in encrypte vorm (bijvoorbeeld minimaal via WinZip met password) naar buiten de GVB omgeving worden gedeeld, of verstuurd. Het berichtenverkeer dient dan onder (code) wachtwoord te worden verzonden (na invoering bestand: onder extra, opties, opslaan, wachtwoord ingeven, ok).
 - e. Interne en externe inbreuken op beveiliging dienen aan de leidinggevende gemeld te worden.
- 5 Bij verlies of diefstal van ICT-Middelen van GVB of van Medewerker met Bedrijfsgegevens, zal ondergetekende direct de GVB Privacy Officer op de hoogte brengen en in overleg aangifte doen bij de politie (meldpuntdatalek@gvb.nl).
Verlies of diefstal van ICT-Middelen altijd melden bij ICT (servicedeskict@gvb.nl) i.v.m. herbestelling van de vervanging.
Bij verlies of diefstal van mobiele telefoons die voorzien zijn van “wipe-functie”, behoudt GVB zich vanwege het risico op datalekken het recht voor om deze onbruikbaar te maken voor verder gebruik. Daarbij zullen bedrijfs- en overige voorkomende gegevens niet meer te benaderen zijn.

- 6 Bij het vermoeden van hacking of ransomware, waarbij bestanden waarmee Medewerker werkte niet meer bereikbaar zijn, of onleesbaar zijn, of waarover een bericht is binnengekomen dat zulke schade zich heeft voorgedaan wordt Medewerker gevraagd om dit onmiddellijk melden bij de ICT Service Desk (servicedeskict@gvb.nl) en onmiddellijk het apparaat uit te zetten en te ontkoppelen. Dit om verdere schade door verspreiding van de malware en het steeds lastiger maken van het herstel, zoveel mogelijk te beperken.
- 7 Het verstrekken van persoonsgegevens aan derde partijen dient zorgvuldig te gebeuren en zowel voor de beveiligings- als voor privacy aspecten gemeld te worden bij de privacy officer. Bijvoorbeeld bij het gebruik van openbare netwerken dienen beveiligingsmaatregelen getroffen te worden vanwege het risico van kennisname of gebruik door onbevoegde derden. Zo ook dient met de ontvangende partij afspraken gemaakt te worden, eventueel met een bewerkersovereenkomst, over de doeleinden van gebruik, te treffen beveiligingsmaatregelen en het vaststellen van een uiterste termijn voor het bewaren en vernietigen van gegevens.

Gebruikersovereenkomst behorende bij het ICT-Protocol

GVB stelt aan ondergetekende, voor door GVB ter beschikking gestelde doeleinden, ICT-middelen ter beschikking ten behoeve van de uitoefening van diens functie.

ICT-middelen die door GVB ter beschikking zijn gesteld, zijn in het bezit van en in licentie bij GVB; GVB treedt zelf op als interne provider.

Ondergetekende zal op een zakelijke, redelijke en zorgvuldige wijze werkzaamheden in het kader van de functie bij GVB uitvoeren. Voor de uitvoering van werkzaamheden bedient ondergetekende zich van ICT-middelen, met inachtneming van wet en regelgeving (strafrechtelijke bepalingen, privacy bescherming etc.), en op een professionele en ethische wijze, passend binnen de onderneming van GVB.

Ondergetekende draagt zelf de verantwoordelijkheid voor het juiste gebruik van ICT-middelen. Het gebruik kan onderwerp van onderzoek zijn in een civiel- en/of strafrechtelijke procedure. Ondergetekende is ermee bekend dat testsituaties met betrekking tot registratie van en controle op het gebruik van ICT-middelen door GVB kunnen plaatsvinden.

Ondergetekende is ervan op de hoogte dat het verwijderen van berichten en gebruikershistorie niet betekent dat deze informatie ook in het geheel uit het geheugen van computer en voicemail zijn verwijderd; het netwerk waarop ondergetekende dan wel ontvanger zijn aangesloten, kent back-up/geheugensystemen.

Te allen tijde zal bij het gebruik van internet, e-mail, telefoon en computerapparatuur zorgvuldigheid betracht worden opdat de vertrouwelijkheid van gegevens en de integriteit en goede naam van GVB gewaarborgd blijven.

Ondergetekende is zich ervan bewust dat ontwikkelingen op het gebied van ICT-middelen GVB ertoe kunnen bewegen veranderingen in bestaande gebruikersmogelijkheden door te voeren.

Ondergetekende is bekend dat bij vermissing door opzet of bewuste roekeloosheid verplichting tot schadevergoeding kan worden opgelegd.

Ondergetekende in dienst van GVB / te werk gesteld in afdeling, verklaart bekend te zijn met de inhoud van dit protocol, een kopie van het onderhavige protocol te hebben ontvangen en zal te allen tijde overeenkomstig het protocol handelen.

Getekend: Amsterdam dd. ...-...-.... Medewerker.....

Leidinggevende naam:..... handtekening.....

De ondertekende gebruikersovereenkomst wordt in het personeelsdossier bewaard.