Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Gedragsregeling voor de digitale werkomgeving [Algemene Versie]

Versie	1.0
Datum	September 2021
Status	Definitief

Inhoud

Inleiding

Zonder informatie kunnen we ons werk niet doen. Delen van informatie binnen en buiten de overheid hoort daarbij. Die informatie moet dan wel correct, actueel en natuurlijk ook vindbaar zijn.
De overheid heeft een publieke taak en transparant zijn naar de samenleving is een kernwaarde. We maken informatie waar mogelijk openbaar en geven inzicht in besluitvorming.
Als je goed omgaat met informatie draag je dus bij aan de betrouwbaarheid, controleerbaarheid en zorgvuldigheid van de rijksoverheid. Burgers en bedrijven verwachten dit ook van ons.

Belangrijke bijkomende aspecten zijn informatiebeveiliging en privacy. We zijn erg afhankelijk van informatie en we werken met persoonsgegevens en andere vertrouwelijke informatie. Het tijdstip waarop en de plek waar we werken is steeds flexibeler. Daarnaast zijn we steeds vaker een doelwit van cybercriminelen met geavanceerde digitale aanvallen gericht op spionage, sabotage en zelfs terrorisme. Zorgvuldig omgaan met informatie betekent dus ook veilig en privacy-verantwoord.

Ons gedrag is dus van groot belang. Met technische en organisatorische maatregelen beperken we al veel risico's, maar dat is niet voldoende. Deze gedragsregeling beschrijft wat je kunt doen om goed om te gaan met informatie zodat die volledig, actueel en vindbaar is en wat je kunt doen om te zorgen dat die informatie veilig en de privacy gewaarborgd blijft. Als we met zijn allen deze regels toepassen, kunnen we beter ons werk doen en worden we digitaal weerbaarder.

Het past bij de eed of belofte waarin je hebt toegezegd om je te gedragen zoals 'een goed ambtenaar betaamt'. Het past ook bij de betrouwbaarheid die de maatschappij van de overheid verwacht. Je houden aan deze regels is dus niet vrijblijvend; die plicht volgt ook uit wet- en regelgeving zoals de Archiefwet, AVG, Voorschrift Informatiebeveiliging Rijksdienst en BIO. Een fout maken of je vergissen kan iedereen overkomen, maar bij opzet en nalatigheid kan het leiden tot personele maatregelen.

De opbouw van het document is als volgt:
- positionering van het document waaronder de scope;
- goede omgang met informatie;
- beveiligingsaspecten in verschillende werksituaties: op kantoor, thuis, onderweg;
- privacy-aspecten;
- omgang met risico's zoals cybercriminaliteit.

Het document eindigt met enkele bijlagen, waaronder een overzicht van gerelateerde documenten. Naar deze documenten wordt in de tekst verwezen met een getal tussen vierkante haken, bv [1].

Laten we er met elkaar voor zorgen dat informatie volledig, actueel en vindbaar is en dat we op een veilige en verantwoorde manier werken. Zo kunnen incidenten worden voorkomen. Help elkaar hierbij zoveel mogelijk. Zo dragen we bij aan de betrouwbaarheid van de Rijksoverheid.

1 Positionering en scope

1.1 Scope

Deze gedragsregeling gaat vooral over digitale informatie en informatiesystemen. Het gaat daarbij om het werken met informatie zodat die volledig, actueel en vindbaar is. En het gaat ook om een veilige en privacy verantwoorde manier van werken. Digitaal werken raakt aan het werken met papieren informatie en fysieke beveiliging. Die onderwerpen komen beperkt aan bod.

Deze gedragsregeling geldt niet alleen voor Rijks- en Defensieambtenaren maar voor alle leidinggevenden en medewerkers die voor de Rijksoverheid werkzaamheden uitvoert en daarbij gebruik maakt van de digitale werkomgeving van de Rijksoverheid. Dit zijn de eigen medewerkers en ook uitzendkrachten en andere externen, medewerkers van zakelijke partners, stagiaires, trainees en vrijwilligers. Deze groep wordt verder aangeduid met (rijks)medewerkers.

Dit document beperkt zich tot regels die voor iedere medewerker gelden. De volgende zaken vallen buiten scope:
- regels voor staatsgeheime informatie, inclusief bedreigingen door statelijke actoren en georganiseerde misdaad;
- specifieke regels voor reizen naar risicolanden;
- informatie waarvoor andere bijzondere regels gelden, zoals medische informatie.

Deze situaties vergen heel specifieke regels die op een klein deel van ons van toepassing zijn.

1.2 Gerelateerde documenten

De regels in dit document zijn gebaseerd op vastgesteld beleid. Dit document vervangt alle gedragsregelingen op het gebied van de digitale werkomgeving van voor 2017. Hierop gelden twee uitzonderingen:
- *Gedragscode Integriteit Rijk [1]*: Dit omvat afspraken op het gebied van integriteit en helpt bij het maken beslissingen op dit gebied.
- *Handreiking Online Communicatie Rijksambtenaren [2]*: hierin staat hoe je integer en professioneel gebruik maakt van online voorzieningen waaronder social media.

Voor werkinstructies, handleidingen en dergelijke wordt naar achterliggende documenten verwezen (zie bijlage 3).

1.3 Eigen versie van de gedragsregeling

Organisaties binnen de Rijksoverheid kunnen een eigen versie van de gedragsregeling digitale werkomgeving uitbrengen:

- In de bijlagen kunnen organisaties aanvullingen doen voor de eigen contactpersonen, voorzieningen en verwijzingen.
- Organisaties binnen de rijksoverheid kunnen in samenspraak met hun medezeggenschap ook aanvullende (zwaardere) regels vaststellen (lichter is niet toegestaan), bijvoorbeeld omdat de organisatie veel vertrouwelijke informatie verwerkt of omdat de organisatie extra gevoelig is voor incidenten en negatieve berichtgeving in de media.

Als een organisatie een eigen versie maakt, wordt de naam van de organisatie toegevoegd in de titel op de voorpagina.

1.4 Personele processen

Iedere rijksmedewerker is zelf verantwoordelijk voor zijn eigen gedrag en de keuzes die hij maakt. Het aan de gedragsregeling houden is belangrijk en niet vrijblijvend [23]. Fouten en vergissingen maken is menselijk. Maar je niet aan deze regels houden kan een blijk zijn van disfunctioneren, plichtsverzuim en niet-integer gedrag.

Als een rijksmedewerker zich niet aan de gedragsregels houdt, kan dat diens leidinggevende aanleiding zijn om dat te bespreken. Dit kan leiden tot nadere afspraken, een training en bij ernstiger situaties tot een aantekening in je personeelsdossier en integriteitonderzoek [24]. Dit is iets tussen jou en je leidinggevende en loopt via de daarvoor vastgestelde procedures.

1.5 Beheer van het document

Voortdurend komt er nieuwe wet- en regelgeving, zoals de Wet Open Overheid (Woo) en de nieuwe Archiefwet. En ook zijn er programma's zoals Hybride werken, Ambtelijk Vakmanschap en Verbetering Informatiehuishouding (IHH). Deze leiden tot nieuwe en vernieuwde gedragsregels. Het is daarom belangrijk dat het document actueel blijft. Dit geldt ook voor verwijzingen naar de achterliggende documenten. Er zijn twee type wijzigingen op dit document:

- Wijzigingen waarbij hoofdregels, zie het overzicht vanaf pagina 25, veranderen. In dat geval veranderen de regels en is brede afstemming noodzakelijk en hernieuwde instemming van de GOR Rijk. Voor Defensie loopt dit via Centrale medezeggenschapscommissie Defensie;
- Tekstuele wijzigingen waarbij een toelichting, een link of een voorbeeld wordt aangepast. Deze wordt vastgesteld door de CIO rijk en gaat ter informatie naar het CIO-beraad en de GOR Rijk.

2 Omgaan met informatie: goed en vindbaar

2.1 Wees open en transparant

Maak informatie openbaar volgens de afspraken binnen jouw organisatie.
De overheid heeft een publieke taak en daarbij zijn openheid en transparantie naar de maatschappij kernwaarden. Dit doen we als overheid vanuit onszelf en ook naar aanleiding van wetgeving zoals de Wob (Wet openbaarheid van bestuur) en de privacywetgeving.
Openbaar maken is dus belangrijk en moet zorgvuldig gebeuren zodat die informatie betrouwbaar is [3]. Het is dus niet de bedoeling dat je zelf informatie over je werk op het internet zet of vragen van journalisten beantwoordt. Iedere organisatie heeft hiervoor regels en procedures opgesteld. Hier zijn vaak juristen, beleidsmedewerkers, woordvoerders en communicatiespecialisten bij betrokken [4].

2.2 Opslaan van informatie: maak het vindbaar

Sla informatie op zodat jij en anderen kunnen terugvinden: op de juiste locatie en met een duidelijke naam.
Informatie slaan we op zodat jij en je collega's deze weer kunnen terugvinden en opnieuw kunnen gebruiken. Collega's kunnen niet bij informatie in jouw mailbox, je persoonlijke schijf of op je telefoon.
Maak intern afspraken over het opslaan van informatie, bv over naam van het bestand, het onderwerp, versienummer, auteur e.d. Gebruik de Rijkshuisstijl bij het opstellen van documenten: die hebben een plek voor dergelijke informatie. Documenten sla je op de gedeelde netwerkschijf op of in een 'document-managementsysteem' (DMS) zoals DigiDoc en DigiJust. [5]. Hiermee voorkom je tijdrovende speurtochten naar informatie.

Ga je binnenkort uit dienst? Draag je werkzaamheden en je informatie op tijd over. Als je steeds je informatie goed opslaat, is dat zo gebeurd!

Werk je met personeelsdossiers? Tip: werk die één voor één af, dan voorkom dat stukken van de één in het dossier van de ander komen.

Je persoonlijke schijf gebruik je voor persoonlijke informatie die niet voor anderen bedoeld is.

2.3 Houd je samenwerkruimtes en netwerkschijven netjes

Maak afspraken over wie en hoe je samenwerkingsruimtes en netwerkschijven netjes houdt.

Voorkom verweesde netwerkschijven en samenwerkruimtes, waar niemand zich verantwoordelijk voor voelt. Spreek (intern) met elkaar af waar je de informatie opslaat, op welk moment en vooral wie de informatie in het archief deponeert als de samenwerking eindigt. Met name wanneer in tijdelijke projecten en samenwerkingsverbanden dossiers ontstaan, wordt het deponeren naar het archief vaak vergeten.

Werk je in groepsverband intensief aan een document met daardoor veel versies? Tip: neem de datum op in de naam van het document.

2.4 Bestempel informatie als vertrouwelijk

Rubriceer en merk je documenten: ontvangers zien dan dat een document (extra) vertrouwelijk is.
Zorg dat je weet wat het belang van de informatie die je hanteert. Sommige informatie is gevoelig en mag alleen in kleine kring gedeeld worden. Geef vertrouwelijke documenten een rubriceringsniveau en/of een merking mee. In de Rijkshuisstijl [5] kan je dit aangeven.
Benoem het eventueel ook nog aanvullend in de tekst van een mail. Hierdoor weten de ontvangers van informatie dat de inhoud (extra) vertrouwelijk is. Ze kunnen dan zelf ook passende maatregelen nemen.

Op zoek naar de Rijkshuisstijlsjablonen? Tip: Deze zijn vaak onderdeel van de werkplek bv als menu in Word of als menu-item via het Windows-logo.

Vraag de afzender of je gerubriceerde of gemerkte informatie mag delen.
Als je informatie ontvangt die gerubriceerd of gemerkt is, gelden daar extra maatregelen voor. Doorgaans mag je niet zelf besluiten om die informatie met een ander te delen. Toch kan het voor het werk nodig zijn om deze informatie te delen met een collega. Vraag dan toestemming aan de afzender.

2.5 Archivering

Archivering gebeurt niet altijd vanzelf. Weet wat jij actief moet doen in het archiveringsproces.
De overheid is eigenaar van alle informatie die de overheid produceert of ontvangt bij het uitvoeren van haar taken. Informatie van de overheid valt onder de Archiefwet: documenten, informatie in applicaties, email, WhatsApp, sms en papieren post. Met de archiefwet en selectielijsten wordt vastgesteld hoe lang we informatie minimaal bewaren. Dit verschilt per proces, applicatie en het type document. Archiveren wordt in bepaalde gevallen automatisch geregeld. Dit geldt bijvoorbeeld voor informatie in applicaties. In andere gevallen moet je zelf een actieve rol hebben. Dit geldt vaak voor documenten op het netwerk. Zorg daarom dat je weet

hoe archivering werkt binnen jouw organisatie en wat je zelf actief moet doen. Op deze manier voldoen we aan de vereisten van volledigheid, toegankelijkheid en beschikbaarheid.

2.6 Respecteer intellectueel eigendom

Voor informatie en afbeeldingen die je van het internet of andere media haalt, gelden drie regels:

- *Pas bronvermelding toe;*
- *Gebruik zoveel mogelijk rechtenvrij materiaal;*
- *Schaf waar nodig betaald materiaal aan.*

Op het internet staat veel informatie, filmpjes, muziek en afbeeldingen die voor het werk nuttig zijn. Dit materiaal kan beschermd worden door het auteursrecht.
Soms is materiaal rechtenvrij en mag je dat gratis gebruiken met bronvermelding. In zoekmachines zoals Google, kan je je resultaten daarop filteren.
Via de Mediatheek Rijksoverheid is het ook mogelijk om beeldmateriaal op te vragen. Zij beheren overeenkomsten met beeldbanken [6].
Als je het toch beschermd materiaal nodig hebt, moet je het laten aanschaffen.

2.7 Help elkaar

Voorkom incidenten: help elkaar, stel vragen en maak de ander bewust de goede omgang met informatie.
In de drukte van alle dag is het makkelijk om iets te vergeten en een fout te maken. Help elkaar bijvoorbeeld door de computer voor de ander te vergrendelen en vertel hem dat als hij er weer is. Verwijder een mailtje dat niet voor jou bedoeld is en meldt dit bij de afzender. Als je denkt dat een collega niet weet hoe hij iets moet doen, laat het een keer zien.
Door elkaar op die manier te helpen, voorkomen we dat zaken misgaan. Als je dit lastig vindt, zijn er natuurlijk ook andere mogelijkheden om iets aan te kaarten, zoals dit melden bij je leidinggevende of een vertrouwenspersoon.

3 Veilig werken op kantoor

3.1 Gebruik de zakelijke ICT-voorzieningen

Gebruik zakelijke ICT-voorzieningen om je werk uit te voeren.
Om je werk te kunnen doen, krijg je toegang tot informatie, applicaties en ICT-voorzieningen. Als je iets mist, kan je aanvullende zaken aanvragen via je leidinggevende. In bijlage 1 staat een overzicht van veilige ICT-voorzieningen. Jouw eigen organisatie heeft mogelijk (ook) andere voorzieningen en regels rond het gebruik van eigen apparatuur: vraag daarnaar bij de servicedesk, je collega's of je leidinggevende. Commerciële voorzieningen toepassen, kan risico's met zich meebrengen (zie 8.4).

3.2 Wachtwoorden: maak het anderen niet te gemakkelijk

Leen je account en wachtwoord niet uit en gebruik wachtwoorden die niet makkelijk te raden zijn.
Je krijgt toegang tot ICT-voorzieningen op basis van een persoonlijke gebruikersnaam. Je account en wachtwoord zijn van jou en die leen je niet uit. Dit geldt ook voor je toegangspas, zoals de Rijkspas, om toegang te krijgen tot gebouwen. Jij bent verantwoordelijk voor wat er met jouw account wordt gedaan.

> Ben je nieuwsgierig hoe veilig onze voorzieningen zijn? Op eigen houtje hacken mag niet. Tip: ga op zoek naar teams die dit als taak hebben. Die zijn altijd op zoek naar enthousiaste collega's!

In bepaalde situaties, zoals bij thuiswerken, moet je ook een 2-factor authenticatie gebruiken [8]. Je gebruikt naast je wachtwoord een tweede middel, bijvoorbeeld een sms-code, om je te identificeren. Hierdoor kunnen anderen niet in jouw account te komen.

Veel wachtwoorden? Gebruik een wachtwoordenkluis.
Er zijn nog diverse voorzieningen en applicaties met een eigen wachtwoord. Al die wachtwoorden onthouden is moeilijk. Veel rijksorganisaties hebben daarom een 'wachtwoordenkluis' zoals KeePass. [9] Hierin kan je alle wachtwoorden veilig opslaan. Ook kunnen die wachtwoorden voor je bedenken zodat je steeds andere wachtwoorden gebruikt.

3.3 Weg van je werkplek: opgeruimd staat netjes!

Vergrendel je computer, laptop, tablet of telefoon.
Vergrendel als je apparatuur als je wegloopt van je (thuis) werkplek. Zo voorkom je dat een bezoeker, collega of huisgenoot toegang krijgt tot jouw email, documenten en systemen (voorbeeld P-Direkt). Je zakelijke telefoon en tablet vergrendel je door kort op de aan/uitknop te drukken. Hoe je je de computer en laptop vergrendelt, varieert:

- via het slotje in je scherm;
- via ctrl+alt+del en daarna de spatiebalk;
- via de toetscombinatie Windowslogo + L

Eenmaal terug op de werkplek, kun je na het intypen van het wachtwoord of de pincode weer verder.

Berg papieren op in een gesloten lade, locker of kast.
Als je een langere tijd van je (thuis)werkplek weggaat, berg dan papieren op in een gesloten lade, locker of kast. Daarmee voorkom je dat een bezoeker, collega of huisgenoot toegang krijgt tot die documenten. Op flexplekken zorg je zo dat je collega aan een opgeruimd bureau kan werken.

3.4 Privégebruik zakelijke ICT-voorzieningen

Hou privégebruik van zakelijke ICT-voorzieningen beperkt.
Beperkt privé gebruik van ICT-voorzieningen is toegestaan. De voorwaarde is dat het je eigen werk en dat van je collega's niet hindert. Sommige rijksorganisaties hebben hiervoor aanvullende regels.

Stuur je een privé mailtje of sla je een privé document op, op het werk? Tip: zet deze in een aparte map 'Prive': dan is dit duidelijk voor je collega's en bij een formeel informatieverzoek.

Surf bewust: blijf weg bij riskante sites
Het bezoeken van sommige sites is op het werk niet toegestaan, ook niet beperkt. Dit betreft bijvoorbeeld pornografische, extremistische, terroristische en goksites. Integriteit is een grondhouding en is een belangrijk onderdeel van de manier waarop je je functie uitoefent [1]. Blijf dus weg bij dergelijke sites.
Sommige sites zijn om andere redenen ongewenst. Op het internet komen ook malafide websites voor, bijvoorbeeld waar je gratis films, muziek en software kan krijgen. Je loopt daar extra risico's op virussen en je kan auteursrechten schenden (zie 2.5).

3.5 Gevonden printjes: ruim ze voor elkaar op

Printjes bij de printer: geef ze aan de eigenaar of gooi ze in de papiercontainer.
Ook als je met je toegangspas print, kunnen printjes langere tijd bij de printer liggen. Dit kan komen door vergeetachtigheid, door een printerstoring of door verzending naar de verkeerde printer.
Geef gevonden printjes aan de eigenaar of gooi ze in de beveiligde papiercontainer. Die staat meestal in dezelfde ruimte als de printer.

Loopt de printer vast? Tip: verwijder de opdracht via het lokale menu van de printer.

3.6 Incidenten: meld en los op

Als je een beveiligingsincident veroorzaakt, meld dit en help waar mogelijk bij het oplossen.
Fouten maken en je vergissen is menselijk. Je kunt bijvoorbeeld klikken op een verkeerde link in een mailbericht, een document achterlaten in het OV of je telefoon kan worden gestolen. Fouten maken kan, ervan leren moet.

Als er iets misgaat of dreigt mis te gaan, (1) meld je dit en (2) los je het op/laat je het oplossen.
Hoe dit werkt, verschilt per organisatie en is afhankelijk van het type incident. In bijlage 2 staan de gegevens voor contactpersonen en de servicedesk die gelden voor jouw organisatie.

Je zakelijke toestel gestolen of kwijt? Meld je toestel ook bij Apple of Google als gestolen of zoek [10]

Bij diefstal en verlies van mobiele apparatuur moet je dit melden bij de servicedesk. Soms moet je ook aangifte doen. Overleg dit met je leidinggevende.

4 Veilig samenwerken

4.1 Vertrouwelijke email: hou het intern

Mail vertrouwelijke informatie alleen naar Rijksmedewerkers.
Binnen de rijksoverheid kunnen we veilig mailen, omdat we de informatie over een beveiligd netwerk sturen. Buiten de rijkoverheid is dat niet het geval. Mail die over het internet verstuurd wordt, is niet beveiligd tenzij je extra maatregelen neemt. Stuur dus geen vertrouwelijke informatie via het internet.

Stuur geen mail naar je privé mailadres.
Ook deze mail is onderweg niet beveiligd. Bovendien is privé-apparatuur in het algemeen niet veilig genoeg. Stuur dus geen mail naar huis, maar maak gebruik van de thuiswerkvoorziening, de zakelijke tablet of de samenwerkruimte [11]. Stuur dus ook niet (standaard) vergaderverzoeken naar je privé-mailadres.

Kies het juiste mailadres.
Een tikfout is zo gemaakt en namen worden in de mail aangevuld. Let dus op naar wie je mail stuurt. Gaat het toch mis en betreft het vertrouwelijke informatie? Meld dit als incident, vraag die persoon het mailtje direct te verwijderen en dat te bevestigen.

> Bij het intypen van een mailadres wordt de naam automatisch aangevuld. Soms staat hier een oud of verkeerd mailadres.
> Tip: ga achter dat mailadres staan en klik op het kruisje: dan komt die niet meer terug.

Versleutel documenten.
Mail je toch vertrouwelijke documenten naar een externe zakelijke partner? Versleutel de documenten dan vooraf met een goed wachtwoord. Daar zijn voorzieningen voor zoals 7Zip, Eclips en LUNA [12]. Als je die niet kent of niet goed weet hoe je ze moet gebruiken, vraag een collega om hulp. Andere mogelijkheden om gegevens te delen staan in 4.2 en 4.3.

4.2 Aangetekende papieren post

Aangetekende papieren post is soms een goed alternatief om informatie te versturen.
De papieren post is wettelijk goed beschermd met het briefgeheim. Op schending hiervan staan sancties, waaronder boetes en zelfs gevangenisstraffen. Door informatie aangetekend te versturen, kan papieren post soms een nuttig en veilig alternatief zijn.
In het bezorgproces raakt een poststuk weleens zoek: meld dit als incident (zie 3.6).

4.3 Veilig delen van (grote) bestanden

Wissel (grote) bestanden met de samenwerkruimte of andere veilige voorzieningen.
Gebruik het DMS of de netwerkschijf om bestanden te delen met directe collega's. Dit werkt niet voor collega's elders binnen de overheid of met zakelijke partners. Hiervoor maak je gebruik van de samenwerkruimte. Deze is ook toegankelijk voor partners buiten de rijksoverheid.
Diverse Rijksorganisaties hebben eigen voorzieningen voor bestandsuitwisseling, zoals SecureTransfer [13] en de Bestandenpostbus [14]. Deze hebben niet de risico's van commerciële toepassingen zoals Dropbox en WeTransfer (zie 8.4).
Sommige Rijksorganisaties stellen beveiligde USB-sticks ter beschikking. Die zijn soms een praktisch alternatief. Draag de stick met het bestand dan wel persoonlijk over.

4.4 Berichtenapps en sms: voor informeel gebruik

Sms – alleen voor algemene mededelingen
Sms is steeds minder veilig: de inhoud kan onderschept worden. Voor een tijdelijke beveiligingscode, zoals voor thuiswerken, is het wel geschikt. Gebruik het zelf alleen voor algemene mededelingen die niet vertrouwelijk zijn. Melden dat je iets later bent of 'ik bel je zo terug' als je een telefoontje niet kunt opnemen, is bijvoorbeeld prima.

Berichtenapps - voor informeel gebruik
De inhoud van berichten in en gesprekken met WhatsApp, Signal en Threema zijn veilig en alleen toegankelijk voor de zender en ontvangers. Gebruik berichten-apps alleen voor informele zaken, zoals een interessant artikel delen, een hulpvraag stellen of sparren met collega's. Gebruik ze *niet* voor persoonsgegevens en voor formele zaken, zoals bestuurlijke aangelegenheden: app met beleid maar niet over beleid.
De berichten (en bijlages) staan namelijk alleen lokaal op jouw toestel. Hierdoor kunnen we niet centraal WOB- en AVG-verzoeken beantwoorden en is de informatie niet vindbaar voor anderen.
Voor de berichtenapps is Rijksbreed geen standaard vastgesteld. Sommige rijksorganisaties hebben dit wel gedaan: informeer binnen je organisatie of er specifieke regels zijn [15].

Toch formeel ingezet? Sla het op.
Tijdens een crisis e.d. kunnen berichten-apps toch voor formele zaken zijn ingezet. Sla de berichten op die van belang zijn voor besluitvorming. Gebruik hiervoor de instructies van jouw organisatie [16]. Dit is van belang voor onderzoek en evaluatie achteraf en ook voor Wob-verzoeken.

4.5 Video-vergaderen met de officiële voorzieningen

Gebruik Webex of de videovoorzieningen die jouw organisatie gebruikt.
Overleggen en vergaderen zijn steeds vaker digitaal. Niet iedere voorziening is veilig of gaat zorgvuldig om met jouw persoonsgegevens. Gebruik daarom de voorzieningen die jouw organisatie aanbiedt. Rijksbreed is dit Webex [17] en sommige organisaties hebben ook eigen voorzieningen.

Uitnodiging van een zakelijke partner
Als een betrouwbare externe partner je uitnodigt via een andere voorziening zou dit voldoende veilig moeten zijn. Voor gecontracteerde leveranciers is dit onderdeel van het Programma van Eisen.
Als je twijfelt, kan je het voorstel doen om de vergadering via de voorziening van jouw organisatie te laten lopen. Ook kan je afspreken om heel vertrouwelijke zaken niet te bespreken.

5 Veilig thuiswerken

5.1 Belastbaarheid: let op jezelf en op elkaar

Hanteer vaste werktijden en een aparte werkplek.
Thuiswerken kan leiden tot overbelasting. Werk en privéleven raken met elkaar vervlochten. Alles speelt zich dicht bij elkaar af en soms zelfs in dezelfde ruimte. Als je je niet prettig voelt bij de situatie, bespreek dit dan met je collega's, je leidinggevende, preventie-medewerker of eventueel een vertrouwenspersoon. Het helpt ook om thuis vaste werktijden te hanteren en daarna je apparatuur uit te zetten of uit het zicht te leggen. Het hebben van een aparte werkplek zorgt er ook voor dat je niet de hele dag op één plek zit.

Neem (samen) pauze.
Kom regelmatig los van je scherm. Neem pauze en maak bijvoorbeeld een wandeling. Dit kan eventueel ook met een collega, want contact houden is belangrijk. Ook digitaal kan je samen koffiedrinken. Dan kan je het over andere zaken dan je werk hebben, bijvoorbeeld over hoe het gaat.

5.2 Zorg voor een veilige thuiswerkplek

Bijna alle kantoorwerkzaamheden kan je ook thuis doen. Je kan met je organisatie in gesprek gaan om een Arbo verantwoorde thuiswerkplek in te richten. Thuiswerken brengt ook een verantwoordelijkheid met zich mee. Zorg er bijvoorbeeld voor dat je de werkplek thuis vergrendeld als je wegloopt en belangrijke documenten opbergt. Voorkom bij overleggen dat iedereen kan meeluisteren.

5.3 Gebruik privé-apparatuur: geen zakelijke informatie

Houd zakelijke informatie op zakelijke apparatuur.
Van privé-apparatuur is de veiligheid niet gegarandeerd. Ook is bekend dat deze vaak virussen hebben en andere beveiligingsissues. Zet dus geen documenten via de mail of een USB-stick op je privé-apparaat. Maak gebruik van de zakelijke apparatuur (smartphone, laptops, tablet etc). Wel is het bij de meeste organisaties toegestaan om met je eigen computer gebruik te maken van de thuiswerkomgeving (zoals Flex2Rijk en Connect). In het ontwerp hiervan is rekening gehouden met het gebruik van privé-apparatuur. In sommige organisaties wordt privé-apparatuur breder ingezet. Hiervoor zijn kaders opgesteld. Check wat voor jou van toepassing is.

> Zakelijk en privé: hou je software en virusscanner actueel en voer updates uit.

5.4 Defecte apparatuur: verwijder gegevens

Verwijder zakelijke gegevens voordat je privé-apparatuur laat repareren.

Als je apparatuur laat repareren, verwijder eerst van zakelijke gegevens op het apparaat. Voor zakelijke apparatuur is dit eenvoudig. Je levert het in via de servicedesk en in hun processen wordt dit geregeld. Op privé apparatuur staan als het goed is geen zakelijke documenten maar misschien wel contactgegevens. Verwijder zakelijke informatie voorafgaand aan de reparatie. Doe dit ook als je privé-apparatuur verkoopt of weggooit.

> Wil je gegevens op je mobiele telefoon of tablet verwijderen? Tip: gebruik de optie 'terugzetten naar fabrieksinstellingen'.

6 Veilig werken onderweg

6.1 Veilig mobiel werken met de zakelijke voorzieningen

Je kan je voorzieningen en apparatuur veilig onderweg gebruiken.
Je kan onderweg veilig werken via de thuiswerkomgeving op je laptop, tablet of telefoon. Hiermee kun je je mail bekijken en versturen en kan je bij andere zakelijke informatie.

6.2 Werk digitaal

Print zo min mogelijk en werk zoveel mogelijk digitaal.
Wil je mobiel werken? Doe dit dan zoveel mogelijk digitaal. Als je met geprinte documenten of notitieboekjes werkt, is de kans groter dat je deze verliest en de informatie direct zichtbaar is. Je kunt onderweg inloggen op de digitale werkomgeving op je laptop, tablet of telefoon. De thuiswerkomgeving brengt je naar de veilige omgeving van je organisatie.

6.3 Mail en agenda onderweg: gebruik de tablet

Gebruik de zakelijke tablet of smartphone om thuis of onderweg te mailen.
Met een zakelijke tablet of smartphone kan je mail afhandelen, afspraken bekijken en ook documenten lezen. Hiervoor worden apps gebruikt zoals BlackBerry en Mobile Iron. Dit werkt snel en eenvoudig en je hebt geen laptop nodig. Zeker onderweg is dat heel praktisch. Veel organisaties beschikken over dergelijke mogelijkheden: vraag hiernaar bij jouw organisatie (zie bijlage 1).

6.4 Ongewenst meeluisteren: hou afstand of bel later

Bel je in het openbaar? Houd dan afstand tot anderen of stel het gesprek uit.
In het openbaar luisteren anderen mee, ook bijvoorbeeld in de lift. Let dus op wat je er bespreekt. Zoek een rustig plekje op en houd afstand tot anderen. Ook kan je aan je gesprekspartner voorstellen om het gesprek later te voeren: niet alles heeft haast.

6.5 Ongewenst meekijken: je buren gluren

Zorg dat anderen niet kunnen meekijken op je scherm.
Ga ervan uit dat je buurman in trein, café of andere openbare plekken meekijkt: mensen zijn nieuwsgierig. Als iemand naast of achter je zit, zorg dan dat je geen vertrouwelijke informatie op je scherm hebt staan.

Werk je veel in het OV of in het openbaar? Tip: vraag een privacy-scherm aan, dan kunnen je buren niet meer meegluren.

6.6 Veilig internetverbindingen: vertrouwde wifi of 4G

Werk via vertrouwde wifi, je persoonlijke hotspot of 3G/4G/5G.
In rijkskantoren is gov-roam [18] beschikbaar en sommige rijksorganisaties hebben een eigen veilig wifi-netwerk. Werk daarbuiten via VPN of de 4G-simkaart in je laptop of telefoon. Je kunt ook je telefoon instellen als een wifi-hotspot om daarmee op je laptop te werken. [19].

Verwijder openbare wifi-netwerken na gebruik
Soms moet je toch via een openbaar wifi-netwerk werken (toegang zonder wachtwoord). Het is belangrijk dat je na gebruik het wifi-netwerk weer uit je opgeslagen netwerken verwijderd. [20] Cybercriminelen kunnen namelijk misbruik maken van opgeslagen openbare wifi-netwerken. [21]

6.7 Veilig op vakantie: laat je werk thuis!

Zakelijke mobiele apparaten mee op vakantie? Weet dan waar je op moet letten.

Laat je werkapparatuur thuis.
Als je op vakantie bent, ben je vrij. Het is vaak niet nodig dat je bereikbaar moet zijn. Laat daarom je werkapparatuur thuis. Voor dienstreizen naar het buitenland gelden aparte regels [1].

Buiten Europa: pas op met datagebruik.
Als je in overleg met je leidinggevende toch je zakelijke apparatuur meeneemt op vakantie, pas dan op met datagebruik. Binnen de EU gelden dezelfde voorwaarden als in Nederland. Maar buiten de EU kunnen hoge tarieven gelden. Hou het gebruik dan strikt zakelijk.

7 Omgaan met persoonsgegevens en privacy

7.1 Vaak goed geregeld en bespreek aandachtspunten

Ga ervan uit dat je persoonsgegevens rechtmatig gebruikt. Twijfel je hierover en zie je een risico? Spreek het uit!
We werken dagelijks met persoonsgegevens, d.w.z. gegevens die direct of indirect te herleiden zijn tot een persoon. Dit doen we met een goede reden, bijvoorbeeld om onze wettelijke taken te kunnen uit voeren of voor onze interne processen.

Beoordeel je brieven en CV's van sollicitanten? Tip: Verwijder ze binnen vier weken na afloop van de procedure conform de richtlijn van de AP.

De overheid heeft veel aandacht voor privacy, maar het kan toch voorkomen dat er meer gegevens dan nodig verwerkt worden of dat deze langer dan nodig bewaard blijven. Maak je je hier zorgen over? Bespreek dit dan in je team of vraag het aan een privacy-specialist in je organisatie.

Als je voor je werk persoonsgegevens gebruikt, mag je ze niet zomaar gebruiken voor een ander doel.
Soms lijkt het een goed idee om persoonsgegevens die je al hebt ook voor een iets ander doel inzetten. Dat mag als dat nieuwe doel voldoende past bij het oorspronkelijke doel waarvoor de gegevens zijn verzameld. Om dit te beoordelen, bespreek je dit in je team of met een privacy-specialist.

7.2 Deel en bespreek gedoseerd persoonsgegevens

Deel en bespreek niet meer informatie over personen dan nodig voor je werk en voor het werk van de collega.
Ook zonder privacywetgeving is het vanzelfsprekend dat je zorgvuldig met persoonsgegevens omgaat. Je wilt zelf ook graag dat een ander zorgvuldig omgaat met jouw gegevens. Als het voor je werk en van je collega nodig is om persoonsgegevens te delen en daarover te praten, is dat prima. Echter, deel en bespreek niet meer informatie over personen dan nodig voor dat doel. Met trots en plezier praten over je werk is uitstekend, maar pas op welke (persoons)gegevens je daarbij deelt.

Rapportages bevatten meestal geen persoonsgegevens. Tip: stuur de brongegevens niet mee: die bevatten vaker persoonsgegevens.

7.3 Voorkom datalekken: werk veilig

Pas de regels voor informatiebeveiliging toe, dan bescherm je ook persoonsgegevens en voorkom je datalekken.

Een belangrijk privacy-onderwerp is het goed beschermen van persoonsgegevens. Je moet ze kunnen gebruiken voor je werk, maar anderen moeten er niet zomaar bij kunnen. Door veilig om te gaan met gegevens bescherm je de privacy van burgers en medewerkers. De clean desk policy, de papiercontainer, nadenken wat je bespreekt in de openbare ruimte etc. dragen ook bij aan privacybescherming.

Wat is een datalek? Een datalek ontstaat als de verkeerdere personen toegang, krijgen tot persoonsgegevens en wanneer persoonsgegevens vernietigd worden zonder dat dit de bedoeling is.

7.4 Datalekken melden: klein en groot

Meld een datalek, ook als ze klein zijn, volgens de procedures die gelden binnen jouw organisatie.
Ook als je heel zorgvuldig werkt, kan je toch een datalek veroorzaken. Dit kan ook buiten je schuld zijn als bijvoorbeeld post zoekraakt met daarin persoonsgegevens.
Datalekken zijn informatiebeveiligingsincidenten en moet je melden volgens de procedures in jouw organisatie (zie ook 3.6). Meld wanneer persoonsgegevens bij de verkeerde persoon terecht komt. Doe dit ook als het risico voor de betrokkenen beperkt is. Door consequent te melden, zien we ook waar ruimte is voor verbetering in proces, systeem en instructie. In de verdere afhandeling wordt ervoor gezorgd dat impactvolle datalekken gemeld worden bij de Autoriteit Persoonsgegevens (AP). Het is belangrijk dat je een potentieel datalek direct meldt zodat we deze tijdig kunnen melden bij de AP. Ook is de administratie op orde bij vragen van de AP de administratie op orde.

7.5 Jouw privacy op het werk

Ga naar de servicedesk als je vragen hebt over jouw privacy op het werk.
Op het werk heb je ook recht op privacy, bijvoorbeeld met betrekking tot je mail en je home directory/persoonlijke schijf. Sommige handelingen met ICT worden digitaal gelogd en gemonitord. Het voornaamste doel hiervan is ICT-beheer waaronder het oplossen van verstoringen en het detecteren van dreigingen. Verder kunnen loggegevens worden ingezien met heel goede redenen en via vastgestelde procedures, zoals voor AVG-inzageverzoeken of integriteitsonderzoek. Heb je vragen over je eigen privacy? Stel ze bij de Servicedesk. Als zij jouw vraag niet kunnen beantwoorden, verwijzen ze je door naar de juiste collega.

8 Pas op voor cybercriminelen, let op je gegevens

8.1 Virussen en betrouwbare software

Installeer op je telefoon en tablet alleen maar apps vanuit de Appstore en Playstore.
In de erkende appstores (App Store, Google Play, BlackBerry World, Windows Store, etc.) staan betrouwbare apps. Apps die van andere plekken komen, kunnen virussen e.d. bevatten. Virussen kunnen documenten op slot zetten waardoor organisaties langdurig niet kunnen werken en het herstel daarvan is kostbaar.

Installeer op de laptop alleen software rechtstreeks van de leverancier.
Sommige medewerkers kunnen zelf software op hun computer of laptop installeren. Populaire software kan je overal downloaden en soms krijg je daarbij gevaarlijke extra's. Installeer alleen software die rechtstreeks van de leverancier komt of via een link op de website van de leverancier.

Ondanks dat we goed beschermd zijn en ook als je goed oplet, kan het misgaan. Meld dat (zie 3.6).

8.2 Phishing: trap er niet in!

Laat niet zomaar je gegevens achter. Bij twijfel: neem rechtstreeks contact op met de afzender.
Cybercrminelen willen graag inloggegevens en financiële gegevens (bv. creditcard) van je organisatie. Dit doen ze via phishing: via een link in een mailtje kom je op een website terecht die bijna niet van echt te onderscheiden is. Daar moet je dan inloggen en gegevens achterlaten. Vervolgens ben je je gegevens kwijt en kunnen die misbruikt worden voor identiteitsfraude. Cybercriminelen vallen met phishingmails ook organisaties aan. Er zijn phisingmails die virussen verspreiden en bijvoorbeeld bestanden op slot zetten met losgeld als doel.

> Wil je beter phishingmails leren herkennen. Op het internet is daar veel informatie over. Enkele voorbeelden staan achterin [22]

Klik dus nooit zomaar op linkjes in mailtjes. Als je toch denkt dat het een 'echt' bericht is, klik dan niet op de link, maar ga zelf naar de website en log daar in. Of neem zelf rechtstreeks contact op per telefoon of mail. Phishing kan grote gevolgen hebben voor de organisatie waarin je werkt. Dagelijks worden organisaties door dergelijke software platgelegd en het herstel kost veel tijd en geld.

8.3 Social engineering en Digitale oplichting

Vraagt een collega plotseling om geld? Bel hem!
Cybercriminelen misbruiken je gegevens hebben om geld mee te verdienen. Ze doen zich bijvoorbeeld als jou voor (‘social engineering’) en vragen je vrienden, familie of collega’s om geld. Phishing leidt zo tot digitale oplichting. Als je zo’n bedelbericht (of mail) krijgt, bel die persoon dan op om te controleren of er echt iets aan de hand is of dat hij slachtoffer is van cybercriminelen.

> Cybercriminelen willen je WhatsApp-account overnemen. Tip: stel ‘verificatie in twee stappen’ in via instellingen/account.

8.4 Gratis software en apps kunnen kostbaar zijn

Maak gebruik van de standaard voorzieningen.
Het internet is zoveel mogelijk vrij toegankelijk. Je kan dus gebruik maken van allerlei handige gratis diensten. Handig is niet altijd veilig. Daarnaast kan je zo het eigenaarschap kwijtraken van je gegevens. Maak dus zoveel mogelijk gebruik van de veilige voorzieningen (zie bijlage 1).

Geef je gegevens niet zomaar weg voor een gratis app.
Een gratis dienst is nooit echt gratis: de aanbieders van die diensten moeten ook geld verdienen. Soms is dat simpelweg door reclame-inkomsten. Soms handelen ze in je gegevens en heb je daar bij het installeren van de app toestemming voor gegeven. Geef je gegevens niet zomaar weg voor een handige app, maar denk na of het je dat wel waard is.

> In-app aankopen kunnen veel geld kosten. Tip: zet in de instellingen aan dat je altijd toestemming moet geven voor aankopen.

Overzicht gedragsregels

Wees open en transparant: Maak informatie openbaar volgens de afspraken binnen jouw organisatie

Opslaan van informatie: maak het vindbaar: Sla informatie op zodat jijzelf en anderen deze kunnen terugvinden: op de juiste locatie en met een duidelijke naam.

Houdt je samenwerkruimtes en netwerkschijven netjes: Maak afspraken over wie en hoe je samenwerkingsruimtes en netwerkschijven netjes houdt.

Bestempel informatie als vertrouwelijk
- Rubriceer en merk je documenten: ontvangers zien dan dat een document (extra) vertrouwelijk is.
- Vraag de afzender of je gerubriceerde of gemerkte informatie mag delen.

Archivering: Archivering gebeurt niet altijd vanzelf. Weet wat jij actief moet doen in het archiveringsproces.

Respecteer intellectueel eigendom
Voor informatie en afbeeldingen die je van het internet of andere media haalt, gelden drie regels:
- Pas bronvermelding toe;
- Gebruik zoveel mogelijk rechtenvrij materiaal;
- Schaf waar nodig betaald materiaal aan.

Help elkaar: voorkom incidenten door elkaar te helpen. Stel vragen en maak de ander van regels en gedrag bewust.

Gebruik je zakelijke ICT-voorzieningen voor je werk: ga na welke voorzieningen jouw organisatie heeft**.**

Wachtwoorden: maak het anderen niet te gemakkelijk.
- Leen je account en wachtwoord niet uit en gebruik wachtwoorden die niet eenvoudig te raden zijn.
- Gebruik een wachtwoordmanager om je wachtwoorden veilig in op te slaan.

Weg van je werkplek: zet de boel op slot:
- Vergrendel je computer, laptop, tablet of telefoon.
- Berg papieren documenten op in een gesloten lade, locker of kast.

Privégebruik zakelijke ICT-voorzieningen
- Hou het privégebruik van de zakelijke ICT-voorzieningen beperkt.
- Surf bewust en blijf weg bij riskante sites.

Gevonden printjes: ruim ze voor elkaar op: geef ze aan de eigenaar of gooi ze in de beveiligde papiercontainer.

Incidenten: meld en los op: als je een beveiligingsincident veroorzaakt of ziet, meld dit en help waar mogelijk bij het oplossen.

Vertrouwelijke email: hou het intern
- Mail vertrouwelijke informatie alleen naar Rijksambtenaren.
- Stuur geen mail naar je privé mailadres.
- Versleutel documenten als je buiten de rijksoverheid mailt.

Aangetekende papieren post is soms een goed alternatief voor het digitaal versturen van informatie.

Veilig delen van (grote) bestanden: gebruik samenwerkruimte of andere veilige voorzieningen.

Berichtenapps en sms: voor informeel gebruik:
- Gebruik sms alleen voor algemene mededelingen.
- Gebruik de app alleen voor informele mededelingen en overleg.
- Toch formeel ingezet? Sla het op!

Video-vergaderen met de officiële voorzieningen: Gebruik Webex en de videovoorzieningen die jouw organisatie gebruikt.

Belastbaarheid: let bij thuiswerken op jezelf en op elkaar
- Hanteer vaste werktijden en een aparte werkplek.
- Neem (samen) pauze.

Zorg voor een veilige thuiswerkplek

Gebruik privé-apparatuur: sla geen zakelijke informatie op, maar hou zakelijke informatie op zakelijke apparatuur.

Defecte apparatuur: Verwijder eventuele zakelijke gegevens voordat je privéapparatuur laat repareren.

Veilig mobiel werken onderweg: gebruik gewoon de zakelijke voorzieningen en apparatuur.

Werk onderweg digitaal: werk zo min mogelijk van papier.

Alleen mail en agenda onderweg: gebruik de zakelijke tablet of smartphone.

Bellen in het openbaar: hou afstand tot anderen of stel het gesprek uit.

Werken in het openbaar: zorg dat anderen niet kunnen meekijken op je scherm.

Gebruik veilig internetverbindingen:
- Werk via vertrouwde wifi, je persoonlijke hotspot of 4G.
- Verwijder openbare wifi-netwerken na gebruik.

Veilig op vakantie: laat je werk thuis!
- Laat je werkapparatuur thuis.
- Toch mee? Pas op met datagebruik buiten de EU.

Privacy is vaak goed geregeld: twijfel je hierover en zie je een risico? Bespreek het met je team of leidinggevende. Gebruik persoonsgegevens voor het oorspronkelijke doel en niet zomaar voor iets anders.

Deel en bespreek gedoseerd persoonsgegevens: doe dit zover dat logisch is voor jouw werk en voor het werk van de collega.

Voorkom datalekken: hou je aan de regels voor informatiebeveiliging en dan bescherm je ook persoonsgegevens.

Meld datalekken: gebruik de procedures van jouw organisatie om datalekken te melden. Doe dit ook als het een klein datalek is.

Jouw privacy op het werk: ga naar de servicedesk als je vragen hebt over jouw privacy op het werk: zij helpen je verder.

Voorkom virussen en andere malware:
- Installeer op je telefoon en tablet alleen maar apps vanuit de Appstore en Playstore.
- Installeer op de laptop alleen software rechtstreeks van de leverancier.

Trap niet in phishing: laat niet zomaar je gegevens achter. Als je twijfelt of het echt is, neem dan rechtstreeks contact op met de afzender.

Pas op met digitale oplichters: Vraagt een vriend plotseling digitaal om geld of vertrouwelijke informatie? Bel hem eerst om te checken of het klopt.

Gratis software en apps kunnen kostbaar zijn
- Maak gebruik van de standaard voorzieningen.
- Geef je gegevens niet zomaar weg voor een gratis app.

Bijlage 1 – Veilige voorzieningen

Rijksbrede voorzieningen

Voorziening	Rubricering	Bijzonderheden
Samenwerkingsruimte i-SWF intern	DepV/BBN2	
Samenwerkingsruimte e-SWF extern	DepV/BBN2	
Mail	DepV/BBN2, mits binnen rijksoverheid, zie 4.1	
Mail + Eclips* of LUNA*	DepV of STG-C	
Harde schijf encryptie/ Safeguard*	DepV	
Mobiele telefoon/tablet: Blackberry Work-apps	DepV	
USB-sticks: Ironkey*, datAshur* en Kobil*	DepV	

* op basis van evaluatie door de AIVD, https://www.aivd.nl/onderwerpen/informatiebeveiliging/beveiligingsproducten/geevalueerde-producten, en er moet dus voldaan worden aan de betreffende inzetadviezen.

Organisatie specifieke voorzieningen

Voorziening	Rubricering	Bijzonderheden
[Naam van de voorziening]	*[tot welk niveau biedt het bescherming]*	

Bijlage 2 – Contactgegevens

Servicedesk <eigen organisatie>
- Telefoonnummer
- Mailadres
- Webpagina

Vragen over informatiebeveiliging
- Beveiligingsautoriteit (BVA): <naam, telefoonnummer, mailadres>
- Beveiligingscoördinator (BVC): <naam, telefoonnummer, mailadres>
- Chief Information Security Officer (CISO): <naam, telefoonnummer, mailadres>
- Informatiebeveiligingsfunctionaris/Security Officer: <naam, telefoonnummer, mailadres>
- Security Operations Center (SOC): <naam, telefoonnummer, mailadres>

Vragen over privacy
- Chief Privacy Officer (CPO): <naam, telefoonnummer, mailadres>
- Functionaris Gegevensbescherming (FG): <naam, telefoonnummer, mailadres>
- Privacy Jurist: <naam, telefoonnummer, mailadres>
- Privacy Officer: <naam, telefoonnummer, mailadres>

Vragen over archivering en duurzame opslag
- Archivaris: <naam, telefoonnummer, mailadres>

Vragen over openbaarmaking gegevens en WOB
- Afdeling communicatie: <mailadres, telefoonnummer>
- Coördinator WOB: <naam, mailadres, telefoonnummer>
- WOB-jurist: <naam, mailadres, telefoonnummer>

Bijlage 3 – Verwijzingen naar achterliggende documenten

[1] Gedragscode Integriteit Rijk, https://www.rijksoverheid.nl/documenten/richtlijnen/2017/12/01/gedragscode-integriteit-rijk-gir

[2] Handreiking Online Communicatie Rijksambtenaren https://www.rijksoverheid.nl/documenten/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren

[3] Kenniskaart werken met informatie
Kenniskaart werken met informatie: waarom is belangrijk en wat willen we bereiken: https://www.informatiehuishouding.nl/projecten/medewerker-aan-informatie/Producten+%26+publicaties/instrumenten/2019/09/17/kenniskaart-werken-met-overheidsinformatie

[4] Instructie voor openbaar maken:
Handreiking: Actief openbaar maken doe je zo! | Instrument | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding

[5] Rijkshuisstijl
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/ciscommunicatie/cismiddelen/cishuisstijl/cisrijkshuisstijlgids

[6] Beeldbankfotografie
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/ciscommunicatie/cisrijksbrede_inkoop_van_communicatiediensten_1/cisfotografie/cisfotostock

[7] instructie wachtwoorden, op te vragen bij auteurs.

[8] Instructie flex2rijk: https://www.ssc-ict.nl/documenten/handleidingen/2020/06/08/handleiding---flexibel-werken-met-een-software-token

[9] instructie Keepass: https://www.ssc-ict.nl/documenten/handleidingen/2019/07/09/handleiding-keepass

[10] Instructie voor diefstal/verloren telefoon/tablet
- Apple: https://support.apple.com/nl-nl/HT201472
- Android: https://support.google.com/accounts/answer/6160491?hl=nl

[11] Instructie voor samenwerkruimten:
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4/cissamenwerkruimten&NavigationContext=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4

[12] instructie voor Luna, Eclipse, 7Zip, op te vragen bij auteurs

[13] Instructie Securetransfer: DAP (rijkscloud.nl)

[14] instructie bestandenpostbus: Bestandenpostbus (rijksweb.nl)

[15] Handreiking mbt berichtenapps:
https://www.informatiehuishouding.nl/Producten+%26+publicaties/richtlijnen/2018/02/07/beleidslijn-berichtenapps
https://www.informatiehuishouding.nl/app-met-beleid

[16] Handreiking opslaan chatberichten:
App met beleid; niet over beleid | Rijksprogramma voor Duurzaam Digitale Informatiehuishouding
[17] instructies voor Webex: Rijksportaal (rijksweb.nl),
Best Practices For Working Remotely (webex.com)
Helpcentrum van Webex

[18] Aanvragen WIFI:
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_/ciswifi__rijksbreed_2&NavigationContext=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_ en
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_/cisbzk_turfmarkt

[19] Gebruik hotspot
Instructie voor instellen telefoon als hotspot apple en android en voor verwijderen opgeslagen wifi-netwerken.

- Android: https://www.youtube.com/watch?v=VBriRsmPAds
- iPhone: https://www.youtube.com/watch?v=cSdl6rCIoTk

[20] Instructie verwijderen wifi-netwerken

- Apple: https://www.youtube.com/watch?reload=9&v=qeFYCvcXakA
- Google/Android: https://www.youtube.com/watch?v=50eblYQIF2w

[21] Handreiking mbt Wifi thuis van NSCS:
https://www.ncsc.nl/documenten/publicaties/2019/mei/01/wifi-onderweg-gebruik-een-vpn

[22] Herkennen phishing
https://www.youtube.com/watch?v=Ls0LBmmhOvY en
www.veiliginternetten.nl

[23] Burgerlijk wetboek, Artikel 7:677 en 678
Wetboek-online.nl | Burgerlijk Wetboek Boek 7 | Artikel 677 (wetboek-online.nl) en Wetboek-online.nl | Burgerlijk Wetboek Boek 7 | Artikel 678 (wetboek-online.nl)

[24] Integriteitsschendingen en Baseline Intern persoonsgericht onderzoek na een integriteits- of beveiligingsincident (BIPO): Rijksportaal (rijksweb.nl)