Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Gedragsregeling voor de digitale en fysieke werkomgeving – algemene rijksbrede versie

De basis voor de training digitale weerbaarheid.

Versie	2.0
Datum	oktober 2025

Colofon

Naam	Gedragsregeling voor de digitale en fysieke werkomgeving
Type	Beleid
Status	Definitief
Versie	2.0
Vastgesteld door	SG BZK
Datum vaststelling	3 oktober 2025
Beheer	CIO Rijk
Contact	CISORijk@minbzk.nl

Versiebeheer

Versie	Omschrijving
1.0	Volledig herziene versie, goedgekeurd door CIO-beraad en ICBR. Na instemming GOR Rijk, vastgesteld door SG BZK op1 september 2021
1.01	Onderhoudsversie: referenties van oude naar nieuwe Rijksportaal omgezet, colofon toegevoegd.
1.7	Herziene versie 2024. Ter review
1.8	Reviewcommentaren verwerkt en goedgekeurd in CIO-beraad en ICBR
1.9a, b, c, d	Input verwerkt van GOR Rijk
1.9e	Versie voor instemmingsverzoek GOR Rijk.
2.0	Na instemming GOR Rijk, vastgesteld door SG BZK op 3 oktober 2025

Inhoud

Inleiding **5**

Deel 1 - De gedragsregels

1 De gedragsregels **7**

2 Toelichting op de gedragsregels **9**
2.1 De regels zijn verplicht 9
2.1.1 Hoe wordt op de regels gestuurd 9
2.2 Waar hebben de regels betrekking op? 9
2.2.1 Waar gaat het niet over? 9
2.3 Andere belangrijke documenten 9

Deel 2 - De gedragsregels; waarom en hoe

1 Omgaan met informatie: goed en vindbaar **12**
1.1 Wees open en transparant 12
1.2 Maak overheidsinformatie vindbaar 12
1.3 Hou samenwerkomgevingen netjes 12
1.4 Bestempel informatie als vertrouwelijk 12
1.5 Scheid informatiestromen 13
1.6 Draag bij aan goede archivering 13
1.7 Respecteer intellectueel eigendom 14
1.8 Ga zorgvuldig om met AI en algoritmen 14
1.9 Help elkaar en stel vragen 14

2 Veilig werken op kantoor **15**
2.1 Gebruik de zakelijke ICT-voorzieningen 15
2.2 Wachtwoorden: sterk en uniek, maak het anderen niet te gemakkelijk 15
2.3 Weg van je werkplek: opgeruimd staat netjes! 15
2.4 Hou privégebruik van zakelijke ICT-voorzieningen beperkt 16
2.5 Gevonden printjes: ruim ze voor elkaar op 16
2.6 Incidenten: meld het eerst en los het dan op 17
2.7 Bezoekers – wees een gastheer/vrouw 17
2.8 Het pand in – pas op meelopers 17
2.9 Draag je toegangspas zichtbaar op kantoor 17
2.10 Social media – wees voorzichtig met details 18

3 Veilig samenwerken **19**
3.1 Vertrouwelijke email: hou het intern 19
3.2 De digitale agenda: let op de inhoud 19
3.3 Aangetekende papieren post 19
3.4 Werk veilig digitaal samen 20
3.5 Berichtenapps en sms: voor informeel gebruik 20
3.6 Videovergaderen met de officiële voorzieningen 21
3.7 Persoonlijke voorzieningen en middelen zijn persoonlijk 21

4 Veilig thuiswerken **22**
4.1 Belastbaarheid: let op jezelf en op elkaar 22
4.2 Zorg voor een veilige thuiswerkplek 22

4.3	Gebruik privé-apparatuur: geen zakelijke informatie	22
4.4	Defecte apparatuur: verwijder gegevens	23
5	**Veilig werken onderweg**	**24**
5.1	Veilig mobiel werken met de zakelijke voorzieningen	24
5.2	Werk digitaal	24
5.3	Mail en agenda onderweg: gebruik je tablet of telefoon	24
5.4	Ongewenst meeluisteren: hou afstand of bel later	24
5.5	Ongewenst meekijken: je buren gluren	24
5.6	Veilige internetverbindingen: vertrouwde WiFi of mobiele dataverbinding	25
5.7	Veilig op vakantie: laat je werk thuis!	25
5.8	Op dienstreis: wees voorbereid!	25
5.9	Onderweg: let op je apparatuur	25
6	**Omgaan met persoonsgegevens en privacy**	**26**
6.1	Vaak goed geregeld en bespreek aandachtspunten	26
6.2	Deel en bespreek persoonsgegevens alleen als dat noodzakelijk is	26
6.3	Voorkom datalekken: werk veilig	26
6.4	Datalekken melden: klein en groot	26
6.5	Jouw privacy op het werk	27
6.6	Denk ook aan de privacy van je collega’s	27
7	**Pas op voor cybercriminelen**	**28**
7.1	Virussen en betrouwbare software	28
7.2	Phishing? Tel eerst tot tien!	28
7.3	Pas op voor bijzondere en onverwachte berichten	29
7.4	Gratis software en apps kunnen kostbaar zijn	29
7.5	Druk, dwang en verleiding: zoek hulp!	30
8	**Beheer en implementatie**	**31**
8.1	Doelgroep	31
8.2	Beheer van het document	31
8.3	Uitfaseren andere regelingen en eigen versie van de gedragsregeling	31
8.4	Toegankelijkheid	32
8.5	Rollen, taken en bevoegdheden	32
8.5.1	Medewerker – eigen verantwoordelijkheid	32
8.5.2	Leidinggevende – voorbeeldgedrag, stimuleren en sturen	32
8.5.3	CIO Rijk	32
8.5.4	CIO Departement	33
8.5.5	CISO Departement	33
8.5.6	P&O-adviseur	33
Bijlage 1 – Veilige voorzieningen		**34**
Bijlage 2 – Contactgegevens		**35**
Bijlage 3 – Verwijzingen naar achterliggende documenten		**36**
Bijlage 4 – Verklarende woordenlijst		**38**

Inleiding

Deze gedragsregeling bevat regels waar je je aan moet houden. Goede omgang met informatie is namelijk heel belangrijk. Zonder informatie kan de Rijksoverheid niet functioneren. Het delen van informatie, binnen en buiten de Rijksoverheid, hoort daarbij. De informatie dient correct, actueel en natuurlijk ook vindbaar te zijn. De Rijksoverheid heeft een publieke taak en transparant zijn naar de samenleving is een kernwaarde. Dat betekent dat we informatie zoveel mogelijk openbaar maken. 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.

Informatiebeveiliging en privacy zijn ook erg belangrijk. We werken met persoonsgegevens en andere vertrouwelijke informatie. Het tijdstip waarop, en de plek waar we werken, is steeds flexibeler. Daarnaast is de Rijksoverheid, en jij dus ook als medewerker, een gericht doelwit van cybercriminelen. Zij proberen onze gegevens te stelen en bespioneren en saboteren ons. Zorg dat je bewust bent van dergelijke risico’s, pas je gedrag hierop aan en volg de regels. Met technische en organisatorische maatregelen beperken we risico’s, maar jouw gedrag is dus ook van groot belang.

Deze gedragsregeling beschrijft wat jij kunt en moet doen om goed om te gaan met informatie. Door het naleven van de regels van de gedragsregeling draag je bij aan het realiseren van publieke waarden en het digitaal weerbaar maken van de Rijksoverheid. Deze regels kunnen ook heel nuttig zijn voor thuis.

Het naleven van deze gedragsregeling is een invulling van de eed of belofte waarin je hebt toegezegd om zorgvuldig met informatie om te gaan en gedragsregels te respecteren. Deze regeling is aanvullend op de ‘Gedragscode Integriteit Rijk’ [1]. Het naleven van gedragsregels is niet vrijblijvend. De regels zijn vaak gezond verstand en ook afgeleid van wet- en regelgeving. Een fout maken of je vergissen kan iedereen overkomen, maar bij opzet en nalatigheid kan het leiden tot personele maatregelen.

De gedragsregeling bestaat uit twee delen:

1. Deel 1 bevat de regels en dat is waar je op aangesproken kan worden.
2. Deel 2 bevat de toelichting op de regels. *Waarom* zijn ze van belang. Daarnaast worden er handvatten gegeven die je kunt gebruiken om je aan de regels te houden. Lees dit deel dus ook zorgvuldig.

De inhoud van deel 1 en deel 2 gaat over de volgende onderwerpen:

- goede omgang met informatie;
- beveiligingsaspecten op het werk: op kantoor, thuis en onderweg en bij het samenwerken;
- privacyaspecten;
- omgang met risico’s zoals cybercriminaliteit.

Het laatste hoofdstuk van deel 2, is voor specialisten zoals de CISO's en de P&O-adviseurs. Dat hoofdstuk behandelt zaken zoals doel, scope, uitfaseren van eigen algemene regeling en onderhoud van het document.

Deze gedragsregeling is de basis voor de training digitale weerbaarheid. Die volgt ook in de opbouw de inhoud van deze regeling.

Deel 1 – De gedragsregels

1 De gedragsregels

Hieronder staan de gedragsregels. Deze regels zijn stellig geformuleerd. Het is immers belangrijk dat wij ons er aan houden. Soms kan dat lastig zijn, of loop je tegen moeilijkheden aan. Maak dat vooral bespreekbaar, bijvoorbeeld met collega's of een vakspecialist. Informeer dan waar nodig ook je leidinggevende.

1. Omgaan met informatie; goed en vindbaar

1.1 Wees open en transparant volgens de afspraken binnen jouw organisatie.
1.2 Sla informatie op zodat jijzelf en anderen deze kunnen terugvinden.
1.3 Volg de afspraken van je organisatie over het gebruik van de samenwerkomgevingen.
1.4 Rubriceer je documenten.
1.5 Vermeng geen zakelijke met privé-informatie[1].
1.6 Archiveer volgens de regels.
1.7 Respecteer intellectueel eigendom: vermeld bronnen en schaf materiaal aan als dat nodig is.
1.8 Gebruik bij AI geen persoonsgegevens of vertrouwelijke informatie.

2. Veilig werken op kantoor

2.1 Gebruik alleen de zakelijke ICT-voorzieningen voor je werk.
2.2 Maak je wachtwoorden sterk en uniek en maak waar mogelijk gebruik van 2-factorauthenticatie.
2.3 Weg van de werkplek: vergrendel de computer en telefoon en berg papieren op.
2.4 Hou het privégebruik van de zakelijke ICT-voorzieningen beperkt.
2.5 Gevonden printjes: geef ze aan de eigenaar of gooi ze in de beveiligde papiercontainer.
2.6 Incidenten: meld direct volgens de afspraken binnen je organisatie.
2.7 Meld bezoek aan, haal ze op en breng ze weg.
2.8 Het pand in: laat niemand zomaar meelopen naar het beveiligde deel.
2.9 Draag je toegangspas zichtbaar op kantoor.
2.10 Plaats geen vertrouwelijke zakelijke informatie of details op social media.

3. Veilig samenwerken

3.1 Vertrouwelijke email: hou deze intern en stuur ze niet naar een privémailadres.
3.2 Stel je agenda open waar mogelijk maar neem geen gevoelige bijlages op.
3.3 Gebruik aangetekende post als veilig digitaal delen niet mogelijk is.
3.4 Veilig digitaal samenwerken en delen van bestanden: gebruik de samenwerkruimte of een andere veilige zakelijke voorziening.
3.5 Gebruik berichtenapps en SMS alleen voor informeel gebruik.
3.6 Videovergaderen: gebruik de officiële voorzieningen van jouw organisatie.
3.7 Wachtwoorden en alle persoonlijke zakelijke middelen deel je niet.

4. Veilig thuiswerken

4.1 Voer vertrouwelijke gesprekken alleen op een plek waar anderen (zoals bijvoorbeeld je buren) niet kunnen meeluisteren.
4.2 Gebruik thuis je zakelijke middelen of de thuiswerkomgeving van je organisatie.
4.3 Bewaar geen zakelijke informatie op privéapparatuur.
4.4 Ga met defecte apparatuur naar de servicebalie van je organisatie.

5. Veilig werken onderweg

5.1 Gebruik ook onderweg gewoon de zakelijke voorzieningen en apparatuur.
5.2 Werk onderweg digitaal: werk zo min mogelijk van papier.
5.3 Gebruik de zakelijke tablet of smartphone als je alleen je agenda bekijkt of mailt.
5.4 Bellen in het openbaar: laat anderen niet meeluisteren of stel het gesprek uit.
5.5 Werken in het openbaar: laat anderen niet meekijken op je scherm.
5.6 Gebruik veilige internetverbindingen: vertrouwde wifi, je eigen hotspot of 5G.
5.7 Op vakantie: maak afspraken over het eventueel meenemen van apparatuur en je bereikbaarheid.
5.8 Bereid je voor op een buitenlandse dienstreis of een verblijf in het buitenland: informeer bij je leidinggevende en BVA naar speciale richtlijnen.
5.9 Let onderweg op je apparatuur en laat die niet onbeheerd achter.

6. Omgaan met persoonsgegevens en privacy

6.1 Bespreek twijfels over het gebruik van persoonsgegevens altijd met je team of een privacyspecialist.
6.2 Gebruik alleen persoonsgegevens die je echt nodig hebt voor je werk
6.3 Meld datalekken (klein en groot) conform de procedures van jouw organisatie.
6.4 Wil je een collega noemen of op de foto zetten? Vraag eerst of dat goed is.

7. Cybercriminelen en andere digitale bedreigingen.

7.1 Voorkom virussen en andere malware: installeer op je telefoon en tablet alleen apps vanuit de RijksAppStore, AppStore, Playstore of de eigen store van je organisatie.
7.2 Gebruik alleen de door je organisatie aangeboden software en apps om je werk te doen.
7.3 Controleer onverwachte of verdachte verzoeken altijd via een ander kanaal (bijv. telefonisch).
7.4 Meld phishingpogingen of verdachte handelingen via de richtlijnen van je organisatie.
7.5 Als externe partijen je onder druk proberen te zetten: zoek hulp bij je leidinggevende en de BVA.

2 Toelichting op de gedragsregels

2.1 De regels zijn verplicht

Deze gedragsregeling (deel 1) bevat regels zodat we veilig en betrouwbaar omgaan met overheidsinformatie en zorgen dat de werkomgeving veilig blijft. Het werken volgens deze regels is verplicht. De organisatie waar je werkt dient je de middelen te verstrekken (of je te trainen) om deze regels ook na te kunnen leven.

2.1.1 Wat als ik een probleem heb met het naleven van een regel?

Soms kan dat lastig zijn, of loop je tegen moeilijkheden aan, om je aan de gedragsregels te houden. Maak dat vooral bespreekbaar, bijvoorbeeld met collega's of een vakspecialist. Informeer waar nodig ook je leidinggevende. Je organisatie dient je daarnaast ook van de juiste middelen en kennis te voorzien om op basis van de gedragsregels te kunnen werken.

Hoe wordt op de regels gestuurd?
Je bent zelf verantwoordelijk voor je eigen gedrag en de keuzes die je maakt. Naleving van de regels uit deel 1 (de gedragsregeling) is belangrijk en verplicht [2]. Fouten en vergissingen maken is menselijk en dat kan iedereen overkomen.
Als je je niet aan de gedragsregels houdt, zonder dat daar overleg over is geweest, kan je leidinggevende dat met je bespreken. Dit kan leiden tot nadere afspraken, een training en bij ernstiger situaties tot een aantekening in je personeelsdossier en integriteitonderzoek [3]. Dit is iets tussen jou en je leidinggevende en loopt via de daarvoor vastgestelde procedures.

De gedragsregels worden toegelicht in deel 2. Hier wordt uitgelegd waarom de regels er zijn en hoe je je aan de regels van de gedragsregeling kunt houden. Dit deel is bedoeld als hulpmiddel en bevat geen afdwingbare regels.

2.2 Waar hebben de regels betrekking op?

De regels zijn vooral gezond verstand en zijn ook afgeleid van wet- en regelgeving. Deze gedragsregeling gaat over digitale en de fysieke werkomgeving. Hoe werk je met informatie zodat die volledig, actueel en vindbaar is. Daarbij moet je ook veilig en privacy verantwoord werken. Digitaal werken raakt ook aan papieren informatie en fysieke beveiliging en dat komt ook aan bod.

2.2.1 Waar gaat het niet over?

Het zijn regels die voor iedere medewerker gelden. De volgende zaken dus niet:

- regels voor staatsgeheime informatie, inclusief bedreigingen door statelijke actoren en georganiseerde misdaad;
- specifieke regels voor reizen naar risicolanden;
- informatie met eigen bijzondere regels, zoals medische informatie.

Hiervoor gelden heel specifieke regels die voor een kleine groep collega's gelden.

2.3 Andere belangrijke documenten

Behalve deze gedragsregeling zijn er nog twee documenten met gedragsregels:

- Gedragscode Integriteit Rijk [1] met afspraken op het gebied van integriteit. Deze helpt je bij het maken beslissingen op dit gebied.
- Handreiking Online Communicatie Rijksambtenaren [4]: hierin staat hoe je integer en goed gebruik maakt van onlinevoorzieningen zoals social media.

Je ziet ook cijfers tussen vierkante haken staan, bv [1]. Die verwijzen naar werkinstructies, handleidingen en dergelijke (zie bijlage 3).

Deel 2 - De regels; waarom en hoe

1 Omgaan met informatie: goed en vindbaar

1.1 Wees open en transparant

Maak informatie openbaar volgens de afspraken binnen jouw organisatie.

De Rijksoverheid heeft een publieke taak en daarbij zijn openheid en transparantie naar de maatschappij kernwaarden. Dit doen we als Rijksoverheid vanuit onszelf en ook vanwege de Wet Open Overheid (Woo) en de privacywetgeving.

Openbaarheid en betrouwbaarheid van informatie is belangrijk [5]. Openbaarheid van informatie vindt plaats volgens de regels en procedures die hiervoor Rijksbreed zijn opgesteld. Hier zijn vaak juristen, beleidsmedewerkers, Woo-coördinatoren en communicatiespecialisten bij betrokken [6].

Als de media je rechtstreeks benadert voor informatie of een reactie, verwijs hen naar woordvoering.

1.2 Maak overheidsinformatie vindbaar

Informatie moet je goed opslaan zodat je collega's het eenvoudig kunnen vinden. Regels toepassen om informatie vindbaar te maken is dus belangrijk. Dit gaat bijvoorbeeld over de naam van een bestand, het onderwerp, versienummer, auteur etc. Ook is het van belang dat je documenten opslaat op een gedeelde netwerkschijf of in een 'document-managementsysteem' (DMS) zoals DigiDoc of DigiJust. Je collega's kunnen namelijk niet bij informatie op je telefoon, in je mailbox of je persoonlijke schijf. Hiermee voorkom je tijdrovende speurtochten van collega's naar informatie. Je persoonlijke schijf gebruik je voor persoonlijke informatie die niet voor anderen bedoeld is.

Gebruik de Rijkshuisstijl als je documenten opstelt. Hierdoor zijn documenten eenvoudig herkenbaar als informatie van de Rijksoverheid en bevatten ze ook kenmerken zodat ze beter vindbaar zijn. [7]

1.3 Hou samenwerkomgevingen netjes

Maak afspraken over wie en hoe je samenwerkomgevingen netjes en overzichtelijk houdt.

Voorkom verwaarloosde netwerkschijven en samenwerkruimtes waar niemand zich voor verantwoordelijk voelt. Spreek met elkaar af waar je de informatie opslaat, op welk moment en vooral wie de informatie in het archief opslaat en de samenwerkruimte verwijdert. Als je tijdelijk met elkaar samenwerkt in een project of een crisis is het gemakkelijk om dit te vergeten en is dit extra belangrijk

1.4 Bestempel informatie als vertrouwelijk

Geef aan hoe vertrouwelijk een document is en waarom. Dit noemen we rubriceren en merken. Ontvangers zien dan dat een document (extra) vertrouwelijk is. Zorg dat je weet wat het belang is van je informatie. Sommige informatie is gevoelig en mag alleen in kleine kring gedeeld worden. Geef vertrouwelijke documenten daarom een rubriceringsniveau en/of een merking mee. Gebruik de Rijkshuisstijl: die heeft daar mogelijkheden voor [7].

Wanneer je gevoelige informatie mailt, benoem dan de vertrouwelijkheid in het onderwerp en de tekst van de e-mail. De ontvangers van de e-mail weten dan dat de inhoud (extra) vertrouwelijk is en kunnen zelf zorgen dat de informatie vertrouwelijk blijft.

Als je informatie ontvangt die gerubriceerd of gemerkt is, mag die je niet zomaar delen met collega's. Toch kan dit nodig zijn voor het voor het werk. Vraag dan toestemming aan de afzender.

1.5 Scheid informatiestromen

Je krijgt vanuit je organisatie de beschikking over alle benodigde zakelijke digitale voorzieningen en gebruikersaccounts. Om informatie goed te kunnen beheren is het noodzakelijk dat je privé[1] van zakelijke informatie scheidt.

Uitgangspunt daarbij is dat voor privé informatie privé accounts en middelen worden gebruikt en dat zakelijke communicatie alleen via zakelijke accounts en middelen verloopt. Dit is van belang om vermenging van informatiestromen te voorkomen. Dit is ook belangrijk voor een goede archivering

Door het niet (tijdig) inleveren van de zakelijke ICT middelen, het gebruik van privé middelen voor zakelijke overheidscommunicatie en het meenemen van zakelijke overheidsinformatie bij uitdiensttreding kan een datalek ontstaan. Ga zorgvuldig om met je zakelijke middelen en de informatie daarop. Het is dus niet toegestaan om bij uitdiensttreding of verandering van functie je zakelijk digitale archief mee te nemen buiten de beheerde omgeving van de Rijksoverheid.

1.6 Draag bij aan goede archivering

Met goede archieven maken we informatie duurzaam toegankelijk zodat iedereen, ook burgers, op het juiste moment over de relevante informatie kan beschikken. Archivering gebeurt soms geautomatiseerd, maar niet altijd. Weet wat jij actief moet doen in het archiveringsproces en spreek anderen erop aan als zij hierin steken laten vallen.

De Rijksoverheid is eigenaar van alle informatie die zij produceert of ontvangt bij het uitvoeren van haar taken. Al die informatie valt onder de Archiefwet; documenten, informatie in applicaties, email, chatberichten, sms en papieren post. Met de Archiefwet en selectielijsten wordt vastgesteld hoe lang de overheid informatie bewaart. De bewaartermijn kan verschillen per proces, applicatie en het type document.

Archiveren wordt in bepaalde gevallen automatisch geregeld. Dit geldt bijvoorbeeld voor informatie in bepaalde applicaties. In andere gevallen heb je in het archiveringsproces zelf een actieve rol. 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 en Vraag om hulp bij twijfel. Op deze manier voldoen we aan de vereisten van informatie die vindbaar, beschikbaar, leesbaar, uitlegbaar, betrouwbaar en toekomstbestendig is.

[1] Partijpolitieke informatie wordt gezien als privé-informatie en dient daarom ook gescheiden bewaard te worden.

1.7 Respecteer intellectueel eigendom

Op het internet staat veel informatie, filmpjes, muziek en afbeeldingen die voor het werk nuttig zijn. Dit materiaal kan beschermd zijn door het auteursrecht.

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.

Soms is materiaal rechtenvrij en mag je het gratis gebruiken mits aan de bronvermelding is voldaan. In zoekmachines, zoals Google, kan je je resultaten daarop filteren.

Op de website van de rijkshuisstijl (https://www.rijkshuisstijl.nl/) staan veel afbeeldingen en foto's die vrij van kosten gebruikt kunnen worden.

Via de Mediatheek Rijksoverheid is het ook mogelijk om beeldmateriaal op te vragen. Zij beheren overeenkomsten met beeldbanken en zorgen dat het auteursrecht wordt voldaan [8]. Als je toch beschermd materiaal nodig hebt, moet je het laten aanschaffen.

1.8 Ga zorgvuldig om met AI en algoritmen

Gebruik van AI (kunstmatige intelligentie) en algoritmen biedt interessante voordelen. Verkeerd gebruik kan grote impact hebben. De Rijksoverheid gaat daarom zorgvuldig hiermee om, zeker daar waar het gevoelige informatie zoals persoonsgegevens betreft.
Gebruik daarom geen persoonsgegevens of vertrouwelijke informatie in AI-systemen. Informeer bij je leidinggevende welke regels gelden binnen jouw organisatie.

1.9 Help elkaar en stel vragen

Voorkom incidenten: help elkaar, stel vragen en maak de ander bewust over de goede omgang met informatie. Als je vragen hebt en je kunt het niet in deze gedragsregeling vinden:

- Zoek op het Rijksportaal of het intranet van je organisatie.
- Vraag collega's of je leidinggevende.
- Bij ICT-vragen: vraag de servicedesk.

In de drukte van de 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 je collega dat zodra deze 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 die 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.

2 Veilig werken op kantoor

2.1 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.

Op eigen initiatief je eigen middelen of gratis voorzieningen toepassen, kan risico's met zich meebrengen (zie 7.4). Jouw eigen organisatie heeft mogelijk andere voorzieningen en regels rond het gebruik van eigen apparatuur; vraag daarnaar bij de servicedesk, bij collega's of bij jouw leidinggevende. Gebruik voor zakelijk gebruik de apps of zakelijke omgeving zoals die door je organisatie worden aangeboden. Dit geldt voor al je apparaten, het maakt niet uit of je op een laptop, mobiele telefoon of tablet werkt. Op eigen initiatief gratis voorzieningen toepassen, kan risico's met zich meebrengen (zie 7.4).

2.2 Wachtwoorden: sterk en uniek, maak het anderen niet te gemakkelijk

Gebruik lange wachtwoorden of wachtwoordzinnen die makkelijk te onthouden maar moeilijk te raden zijn. Hoe langer het wachtwoord hoe meer moeite anderen moeten doen om dit wachtwoord te kraken. Gebruik steeds een ander wachtwoord en kies andere wachtwoorden voor je zakelijke en privéaccounts. Meer informatie over het kiezen van een goed wachtwoord is te vinden op het Rijksportaal [9].

Al die wachtwoorden onthouden is lastig. Veel rijksorganisaties hebben daarom een 'wachtwoordenkluis' zoals het programma KeePass [10]. Hierin kan je alle wachtwoorden veiliger opslaan. Ook kunnen die wachtwoorden voor je bedenken zodat je steeds andere wachtwoorden gebruikt. Het gebruik van KeePass of een andere wachtwoordkluis wordt daarom sterk aangeraden.

Steeds vaker kan je ook een 2-factor authenticatie gebruiken. Dit is standaard als je vanaf thuis werkt [11] of een cloudapplicatie gebruikt. Je gebruikt dan naast je wachtwoord een tweede middel, bijvoorbeeld een app op je telefoon, om in te loggen: een dubbel slot. Hierdoor is het moeilijker voor anderen om in jouw account te komen.

Is een wachtwoord toch bij anderen bekend geworden of vermoed je dat; verander dan meteen dat wachtwoord en meld het als een incident bij de servicedesk of je leidinggevende.

2.3 Weg van je werkplek: opgeruimd staat netjes!

Vergrendel je computer, laptop, tablet of telefoon.

Vergrendel al je apparatuur als je wegloopt van je werkplek. Zo voorkom je dat een bezoeker of collega onbedoeld toegang krijgt tot jouw email, documenten en andere systemen. Je zakelijke telefoon en tablet vergrendel je door kort op de aan/uitknop te drukken. Zie je dat een collega vergeten is zijn scherm te vergrendelen, doe dit dan voor hem en meld dat later even.

Hoe je je de computer en laptop vergrendelt, varieert:

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

Doe dit niet alleen op kantoor, maar ook thuis: maak hier een automatisme van. 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 werkplek weggaat, berg dan papieren op in een gesloten lade, locker of kast. Daarmee voorkom je dat een bezoeker of collega onbedoeld toegang krijgt tot die documenten. Op flexplekken zorg je zo dat je collega aan een opgeruimd bureau kan werken.

Op hulpmiddelen als een whiteboard of flip-over kan vertrouwelijke informatie terecht komen. Wis een whiteboard na gebruik en verwijder gebruikte flip-over vellen. Deze vellen kun je opbergen in je persoonlijke locker of weggooien in de daarvoor bedoelde beveiligde papiercontainers.

2.4 Hou privégebruik van zakelijke ICT-voorzieningen beperkt

Op je werk ben je bezig met je werk. Soms moet je hiervan afwijken, bijvoorbeeld om je huisarts te bellen. Ook beperkt privégebruik 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. In de bruikleenovereenkomst van je persoonlijke middelen kunnen hierover richtlijnen opgenomen zijn.

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 jij je functie uitoefent [1]. Blijf dus weg bij dergelijke sites.

Sommige sites zijn om andere redenen ongewenst. Op het internet komen ook onbetrouwbare 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 1.7).

2.5 Gevonden printjes: ruim ze voor elkaar op

Wanneer je printjes bij de printer vindt, geef je deze aan de eigenaar of gooi ze in de papiercontainer.

Tooltip: Loopt de printer vast tijdens het printen? Tip, verwijder de printopdracht uit het menu van de printer: dan wordt deze niet later alsnog afgedrukt als je er niet bij bent.

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.

2.6 Incidenten: meld het eerst en los het dan op

Als je een beveiligingsincident veroorzaakt, meld dit en help waar mogelijk bij het oplossen. Meld liever te vaak dan één keer te weinig. Een informatiebeveiligingsincident gebeurt wanneer vertrouwelijke informatie (bijvoorbeeld wachtwoorden of documenten) in verkeerde handen komt. Of dat iemand toegang krijgt tot een systeem waar dat niet de bedoeling is.

Fouten maken en je vergissen is menselijk. Je kunt bijvoorbeeld per ongeluk 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.

Tooltip: Weet waar je incidenten moet melden, zet de contactgegevens hiervoor in je telefoon en in je favorieten.

Bij diefstal en verlies van persoonlijke ICT-middelen moet je dit melden bij de servicedesk. Soms moet je ook aangifte doen. Overleg dit met je leidinggevende.

2.7 Bezoekers – wees een gastheer/vrouw

Als je op het werk bezoek krijgt, wees dan een goed gastheer/vrouw. Meld ze aan zoals dat bij jullie afgesproken is. Haal ze op en begeleid ze aan het eind weer naar de uitgang. Ook als je een bezoeker zoekend ziet rondlopen, probeer ze te helpen. Dit alles geeft bezoekers het gevoel dat ze welkom zijn en het voorkomt dat ze per ongeluk op verkeerde plekken komen.

Loopt er iemand rond die je niet kent, pas het Sinterklaas-principe toe: ‘het is een vreemdeling zeker, die verdwaald is zeker, ik zal hem even vragen naar zijn naam’

2.8 Het pand in – pas op meelopers

In de kantoorpanden moet je je meestal aanmelden met een bedrijfspas, zoals de Rijkspas. Pas daarna kan je het afgeschermde deel in. Wat kan gebeuren is dat iemand mee probeert te lopen. Laat dit je niet gebeuren. Spreek deze ‘meeloper’ hierop aan en waarschuw de beveiliging zodat die dat kunnen afhandelen.

2.9 Draag je toegangspas zichtbaar op kantoor

Draag op kantoor je toegangspas, zoals de Rijkspas, zichtbaar.

Dit geldt ook voor bezoekers. Aan de toegangspas kan je namelijk direct zien of iemand een collega is of een bezoeker.

Tooltip: Draag je toegangspas niet zichtbaar buiten op weg van of naar kantoor. Je bent dan voor iedereen eenvoudig herkenbaar als rijksambtenaar. Dat kan mogelijk tot ongewenste situaties leiden, bijvoorbeeld bij demonstraties e.d.

2.10 Social media – wees voorzichtig met details

We zien graag dat iedereen trots is op zijn werk en daar over wil vertellen. Werken bij de Rijksoverheid is ook mooi! Informatie delen op social media kan daar onderdeel van zijn. Denk na over welke details je wel en niet deelt op social media. Te veel details delen kan je kwetsbaar maken voor druk van buitenaf (zie 7.5). Dit geldt vooral voor medewerkers in gevoelige functies.

Let bij het delen van foto's ook op de details. Zijn er geen documenten, schermen of whiteboards zichtbaar met gevoelige informatie? Willen eventuele collega's wel op de foto?

In de Gedragscode integriteit Rijk [1] vind je de kaders voor integer gebruik van social media.

3 Veilig samenwerken

3.1 Vertrouwelijke email: hou het intern

Mail vertrouwelijke informatie alleen naar Rijksmedewerkers.

Binnen de Rijksoverheid kunnen we veilig mailen. Buiten de Rijksoverheid is dat niet altijd 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 privémail en wees dus ook voorzichtig met automatisch doorsturen van mail. Ook deze mail is onderweg niet beveiligd. Maak gebruik van de thuiswerkvoorziening, de zakelijke tablet of de samenwerkruimte [12]. Stuur dus ook geen zakelijke 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. Controleer bij twijfel het correcte e-mailadres in de Rijksadresgids. Gaat het toch mis en betreft het vertrouwelijke informatie? Meld dit als incident (zie 2.6) en vraag de ontvanger om het mailtje direct te verwijderen en dat te bevestigen.

Versleutel documenten. Mail je toch vertrouwelijke documenten naar een externe zakelijke partner? Versleutel de documenten dan vooraf met een sterk wachtwoord. Daar zijn voorzieningen voor zoals 7Zip [13]. 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 3.3 en 3.4.

3.2 De digitale agenda: let op de inhoud

Neem geen vertrouwelijke of privacygevoelige documenten op in je agendaverzoeken.

Het is een goed gebruik om je zakelijke agenda te delen met je collega’s. Dat is handig voor het maken van afspraken en maakt het samenwerken eenvoudiger. Hou er rekening mee dat documenten die je in een vergaderverzoek opneemt mogelijk ook zichtbaar zijn voor collega’s die niets met het betreffende onderwerp te maken hebben. Je kan een agenda-item ook als privé markeren, zodat je alleen zelf bij het onderwerp en de inhoud van dit agenda-item kan.

3.3 Aangetekende papieren post

Aangetekende papieren post is soms een goed alternatief om informatie te versturen als digitaal delen niet mogelijk is.

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 2.6).

3.4 Werk veilig digitaal samen

Wissel (grote) bestanden uit met de samenwerkruimte of andere veilige voorzieningen.

Gebruik het documentmanagementsysteem (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.

Tooltip: vind je een USB stick op kantoor of op de parkeerplaats, stop die niet in de computer maar lever die in conform de procedures die gelden in jouw organisatie. Op onbekende USB sticks kunnen virussen en andere kwaadaardige software staan.

Diverse Rijksorganisaties hebben eigen voorzieningen voor bestandsuitwisseling, zoals SecureTransfer [14] en de Bestandenpostbus (JenV) [15]. Deze hebben niet de risico's van de op internet algemeen beschikbare toepassingen (zie 7.4).

Sommige Rijksorganisaties stellen beveiligde USB-sticks ter beschikking. Die zijn soms een praktisch alternatief. Draag de stick met het bestand dan wel persoonlijk over.

3.5 Berichtenapps en sms: voor informeel gebruik

Gebruik SMS alleen voor algemene mededelingen.

SMS is niet veilig omdat sms-berichten niet zijn versleuteld: de inhoud kan gemakkelijk onderschept worden. Gebruik SMS daarom alleen voor algemene mededelingen die niet vertrouwelijk zijn en niet voor inhoudelijke zaken. Melden dat je iets later bent of 'ik bel je zo terug' als je een telefoontje niet kunt opnemen, is bijvoorbeeld prima.

Berichtenapps alleen voor informeel gebruik

De inhoud van berichten en gesprekken met WhatsApp, Signal en Threema zijn veilig en alleen toegankelijk voor de zender en ontvangers. Dit geldt niet voor zogenaamde metagegevens zoals de personen met wie je appt, wanneer je appt en de locatiegegevens. Ook deze gegevens kunnen gevoelig zijn.

Gebruik berichten-apps alleen voor informele zaken, zoals een interessant artikel delen, een hulpvraag stellen of een afspraak in te plannen. Gebruik ze niet voor het delen van persoonsgegevens, medische gegevens zoals ziekmeldingen en voor formele zaken, zoals bestuurlijke aangelegenheden: app met beleid maar niet over beleid. Daarbij is het van belang dat zakelijke berichten (inclusief foto's, video's et cetera) na verzending niet worden verwijderd of aangepast.

De zakelijke chatberichten (en bijlages) staan namelijk alleen lokaal op jouw toestel en zijn niet centraal binnen de organisatie gearchiveerd. Zakelijke chatconversaties vallen zowel onder de Archiefwet, de Wet Open Overheid (Woo) en de AVG. Hierdoor kunnen we heel lastig Woo- en AVG-verzoeken beantwoorden, want dan moeten we per telefoon nagaan welke zakelijke chatberichten en -conversaties daar op staan. Ook zijn deze chatconversaties niet vindbaar voor anderen. Ga daarom bij zakelijk gebruik spaarzaam en bewust met dit middel om.

Voor de berichtenapps is Rijksbreed geen standaard vastgesteld. Sommige rijksorganisaties hebben dit wel gedaan: informeer binnen je organisatie of er specifieke regels zijn [16].

Berichtenapps toch formeel ingezet? Sla het op conform de instructies.

Tijdens een crisis e.d. kunnen berichten-apps toch voor formele zaken zijn ingezet. Sla dan de berichten op die van belang zijn voor besluitvorming. Gebruik hiervoor de instructies van jouw organisatie [17]. Dit is van belang voor onderzoek en evaluatie achteraf en ook voor Woo verzoeken en archivering.

3.6 Videovergaderen met de officiële voorzieningen

Gebruik Webex, Teams of een andere videovoorziening die jouw organisatie gebruikt.

Overleggen en vergaderingen zijn steeds vaker digitaal. Niet iedere voorziening is veilig of gaat zorgvuldig om met jouw persoonsgegevens. Gebruik daarom de voorzieningen die jouw organisatie aanbiedt. De Rijksbrede voorziening hiervoor is Webex [18]. Hiernaast gebruiken veel organisaties Microsoft Teams voor videovergaderingen. Sommige organisaties hebben daarnaast ook nog andere eigen voorzieningen. Als een betrouwbare externe partner je uitnodigt via een andere voorziening zou dit voldoende veilig moeten zijn. Met gecontracteerde leveranciers zijn hier afspraken over gemaakt.

Als je twijfelt, kan je het voorstel doen om de vergadering via de voorziening van jouw organisatie te laten lopen.

Zeer vertrouwelijke zaken bespreek je niet via videovergaderen. Zoek elkaar dan gewoon op.

3.7 Persoonlijke voorzieningen en middelen zijn persoonlijk

Dit geldt voor bijna alle voorzieningen waar je gebruik van maakt. Je krijgt toegang tot ICT-voorzieningen op basis van je gebruikersnaam. Je account, wachtwoord en voorzieningen zijn van jou en die leen je niet uit. Dit geldt ook voor je toegangspas, zoals de Rijkspas, om toegang te krijgen tot gebouwen. Maar ook je laptop, tablet en telefoon worden op persoonlijke basis uitgegeven. Jij bent zelf verantwoordelijk voor wat er met jouw account, E-mailadres, apparaten en voorzieningen wordt gedaan.

4 Veilig thuiswerken

4.1 Belastbaarheid: let op jezelf en op elkaar

Thuiswerken biedt diverse voordelen, maar kan ook een extra belasting geven. Werk en privé raken vervlochten en alles speelt zich af in dezelfde ruimtes. De afstand tot je collega's neemt daarbij toe. Het is van belang dat jij je belastbaarheid in de gaten houdt en dit met je leidinggevende bespreekt. Ook kan je contact opnemen met een preventiemedewerker of een vertrouwenspersoon.

Als je je zorgen maakt over je collega's, bespreek dit met hen of meld het bij je leidinggevende. Neem omgekeerd ook signalen van je collega's serieus.

Tooltip: Hanteer ook thuis vaste werktijden en zet daarna je apparatuur uit. Zorg, als het kan, dat je thuis een aparte werkplek hebt: dan zit je niet de hele dag op één plek.

Neem (samen) pauze. Kom ook thuis regelmatig los van je scherm en neem pauze. Maak bijvoorbeeld (samen) een wandeling of sta elk uur even op en loop door het huis. Maak een (digitale) koffieafspraak met collega's: dan hou je contact en kan je het ook over andere zaken hebben.

Thuiswerken moet niet leiden tot fysieke klachten. Je kunt via je leidinggevende en de preventiemedewerker zorgen voor een Arbo-verantwoorde thuiswerkplek. Zij weten ook welke regelingen en vergoedingen hiervoor zijn. Val je onder de CAO Rijk dan kan je gebruik maken van een werkplekvergoeding en, als dit niet voldoende is, kan je gebruik maken van de IKB-regeling. Zie voor meer informatie het complete overzicht op de website van P-Direkt [19].

4.2 Zorg voor een veilige thuiswerkplek

Thuiswerken brengt ook een verantwoordelijkheid met zich mee. Vergrendel ook thuis je werkplek en berg belangrijke documenten op wanneer je even wegloopt en aan het eind van je werkdag. Voorkom ook thuis dat bij een gevoelig overleg anderen kunnen meeluisteren en doe dit dus niet in de tuin of balkon.

Slimme speakers en andere vormen van digitale assistenten (ook op de smartphone) komen steeds meer voor. Let erop dat deze onbedoeld ook informatie kunnen opvangen. Zet ze uit of op gedempt (mute) als een gesprek vertrouwelijke of privacygevoelige onderwerpen bevat.

4.3 Gebruik privé-apparatuur: geen zakelijke informatie

Hou zakelijke informatie op zakelijke apparatuur. Bij privé-apparatuur is er geen controle op de veiligheid vanuit de ICT-leverancier van de organisatie. Hierdoor is er risico op virussen en andere beveiligingsissues. Zet dus geen zakelijke informatie op je privé-apparaat. Maak zoveel mogelijk gebruik van de zakelijke apparatuur (smartphone, laptops, tablet, etc.) en zakelijke voorzieningen. Zet zakelijke informatie ook niet in je eigen OneDrive, Google Drive of iCloud maar maak gebruik van zakelijke voorzieningen zoals de thuiswerkplek en de samenwerkruimte.

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 van die thuiswerkomgeving is rekening gehouden met het gebruik van privé-apparatuur.

In sommige organisaties wordt privé-apparatuur (nog) breder ingezet. Als dit het geval is, informeert je leidinggevende je hierover met de regels die daarvoor gelden. Heb je hier vragen over, overleg dit dan met je leidinggevende.

4.4 Defecte apparatuur: verwijder gegevens

Op privé-apparatuur kan toch zakelijke informatie staan zoals contactgegevens. Als je privé-apparatuur laat repareren, verwijder dan eerst ten minste de zakelijke gegevens op het apparaat. Doe dit ook als je privé-apparatuur verkoopt of weggooit. Voor zakelijke apparatuur is dit eenvoudig. Je levert het in via de servicedesk en zij regelen dat zakelijke apparatuur wordt opgeschoond.

Tooltip: Wil je gegevens op je mobiele telefoon of tablet verwijderen? Tip: gebruik de optie ‘terugzetten naar fabrieksinstellingen’.

5 Veilig werken onderweg

5.1 Veilig mobiel werken met de zakelijke voorzieningen

Je kan je zakelijke voorzieningen veilig onderweg gebruiken.

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

5.2 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 ook onderweg naar de veilige omgeving van je organisatie.

Werk je thuis of onderweg toch met fysieke dossiers? Ga er dan op dezelfde wijze mee om als op kantoor. Berg ze op als je ze niet gebruikt en vernietig deze indien nodig. Gooi ze niet zomaar in de papierpak thuis.

5.3 Mail en agenda onderweg: gebruik je tablet of telefoon

Gebruik bij voorkeur de zakelijke tablet of smartphone om 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 die veel ruimte nodig heeft. Veel organisaties beschikken over dergelijke mogelijkheden: vraag hiernaar bij jouw organisatie (zie bijlage 2).

5.4 Ongewenst meeluisteren: hou afstand of bel later

Bel je in het openbaar? Hou dan afstand tot anderen of stel het gesprek uit.

In het openbaar luisteren anderen mee, ook bijvoorbeeld in de lift en tram. Let dus op wat, waar en met wie je iets bespreekt. Zoek een rustig plekje op en hou afstand tot anderen. Ook kan je aan je gesprekspartner voorstellen om het gesprek later te voeren: niet alles heeft haast. Dit kan ook relevant zijn op kantoor en thuis: voer je een gevoelig gesprek, zoek dan een geschikte ruimte op en doe ramen en deuren dicht.

5.5 Ongewenst meekijken: je buren gluren

Zorg dat anderen niet kunnen meekijken op je scherm: gebruik een privacyscherm.

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. Ook op kantoor en

Tooltip: Werk je veel in het OV of in het openbaar? Tip: vraag bij je leidinggevende een privacy-scherm aan, dan kunnen andere reizigers niet meer meegluren

thuis kan dit relevant zijn: als je bij een raam zit, kunnen misschien voorbijgangers of buren meekijken en dan doe je dus (rol)gordijnen dicht.

5.6 Veilige internetverbindingen: vertrouwde WiFi of mobiele dataverbinding

Werk via vertrouwde WiFi, je persoonlijke hotspot of 3G/4G/5G.

In rijkskantoren is govroam [20] 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. [21].

Openbare WiFi-netwerken:

Soms moet je een WiFi-netwerk van een andere partij gebruiken. Denk aan het WiFi-netwerk in de trein, restaurant, hotel of camping enz. Je weet niet hoe veilig deze WiFi-netwerken zijn. Bij een minder veilig ingericht netwerk bestaat bijvoorbeeld een risico op het onderscheppen van gegevens of surfgedrag. De thuiswerk- en andere voorzieningen die je organisatie verstrekt zijn hier tegen beveiligd.

5.7 Veilig op vakantie: laat je werk thuis!

Als je op vakantie bent, ben je vrij. Het is vaak niet nodig dat je bereikbaar moet zijn. Laat daarom je werkapparatuur thuis: dan kom je echt tot rust en loop je ook geen onnodige risico’s met je werkapparatuur.

Bij een langer verblijf in het buitenland kan het aantrekkelijk lijken om bereikbaar te zijn of werkzaamheden vanaf dit buitenlandse adres uit te voeren. Overleg dit altijd vooraf met je leidinggevende en de BVA van je organisatie.

5.8 Op dienstreis: wees voorbereid!

Voor dienstreizen naar het buitenland gelden aparte regels [1]. Deze kunnen afhankelijk zijn van het exacte land waar je naartoe gaat. Binnen Europa zijn er doorgaans geen bijzonderheden: onze apparatuur is daarvoor veilig genoeg.

Met Europa wordt hier bedoeld: De landen van de EER, het Verenigd Koninkrijk (Groot-Brittannië en Noord-Ierland), Zwitserland en Caribisch Nederland. Op Rijksoverheid.nl kun je vinden welke landen deel uit maken van de EER [22].

Indien je voor het werk op reis gaat naar een land buiten Europa kunnen er mogelijk speciale richtlijnen gelden. Neem hiervoor tijdig contact op met de BVA van je organisatie.

Pas buiten Europa 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. In de bruikleenovereenkomst van je persoonlijke middelen kunnen hierover richtlijnen opgenomen zijn.

5.9 Onderweg: let op je apparatuur

Tooltip: Moet je spullen toch in de auto achterlaten? Laat die niet zichtbaar liggen, maar leg de laptop vast met een kabelslot in je achterbak of vraag een laptopkluis aan.

Er zijn altijd dieven en anderen die je apparatuur willen stelen. Wanneer je onderweg bent hou dan zicht op je apparatuur en laat die niet onbeheerd achter.

6 Omgaan met persoonsgegevens en privacy

6.1 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!

Iedereen gebruikt in zijn werk persoonsgegevens. Dit zijn gegevens die direct of indirect ter herleiden zijn op een persoon. We gebruiken persoonsgegevens bijvoorbeeld om onze wettelijke taken uit te voeren. Ondanks dat we veel aandacht hebben voor privacy komt het voor dat we te veel persoonsgegevens verwerken, te lang bewaren of delen met iemand die ze niet nodig heeft. Bespreek dit in je team of vraag het na bij een privacyspecialist zoals een Chief Privacy Officer (CPO).

Gebruik persoonsgegevens niet zomaar voor een ander doel.

Soms lijkt het een goed idee om persoonsgegevens in te zetten voor een ander doel. Dat mag alleen als dat hergebruik voldoende past bij het oorspronkelijke doel. Om het hergebruik te beoordelen, bespreek je dit in je team of met een privacyspecialist.

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

6.2 Deel en bespreek persoonsgegevens alleen als dat noodzakelijk is

Deel en bespreek niet meer informatie over personen dan direct nodig voor je werk en voor het werk van de collega. Maak dus altijd gebruik van het principe dataminimalisatie.

Het is vanzelfsprekend dat je zorgvuldig met persoonsgegevens omgaat. Je wilt immers zelf ook graag dat een ander zorgvuldig omgaat met jouw gegevens. Als het voor je werk en het werk 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 van burgers en collega's je daarbij deelt.

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

6.3 Voorkom datalekken: werk veilig

Pas de regels voor informatiebeveiliging toe, dan bescherm je ook persoonsgegevens en voorkom je datalekken! Privacy betekent ook gegevens goed beschermen. Door veilig om te gaan met gegevens bescherm je de privacy van burgers en medewerkers en voorkom je datalekken. De clean desk policy, de papiercontainer, nadenken wat je bespreekt in de openbare ruimte etc. dragen ook bij aan privacybescherming.

6.4 Datalekken melden: klein en groot

Meld ieder datalek, hoe klein dan ook, volgens de procedure van jouw organisatie. Ook als je heel zorgvuldig werkt, kan het voorkomen dat er een datalek optreedt.

Datalekken zijn informatiebeveiligingsincidenten en je moet ze melden volgens de procedures van jouw organisatie (zie ook 2.6). Meld wanneer persoonsgegevens bij een verkeerde ontvanger terecht zijn gekomen en wanneer je informatie of een informatiedrager kwijt bent geraakt. Door jouw meldingen kunnen we ook verbeteringen doorvoeren.

Tooltip: Wat is een datalek? Een datalek ontstaat als informatie (brief, mail) naar de verkeerde persoon is gestuurd en ook wanneer persoonsgegevens vernietigd worden zonder dat dit de bedoeling is.

Meld altijd, ook als je denkt dat het risico klein is. In de verdere afhandeling zorgen we 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. Jouw meldingen zorgen dat onze administratie op orde is bij eventuele vragen van de AP.

6.5 Jouw privacy op het werk

Ga naar de servicedesk of je privacy contactpersoon als je vragen hebt over jouw privacy op het werk.

Privacy is een grondrecht: ook op het werk heb je ook recht op privacy. Dit heeft bijvoorbeeld betrekking je e-mail en je persoonlijke schijf.

Wat je doet met de ICT wordt deels digitaal gelogd en gemonitord. Het voornaamste doel is ICT-beheer. Denk aan het oplossen van storingen en het detecteren van dreigingen. Verder mag je werkgever alleen bij je loggegevens met heel goede redenen en wanneer procedures zijn gevolgd. Voorbeelden hiervan zijn AVG-inzageverzoeken of een 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.

6.6 Denk ook aan de privacy van je collega’s

Op kantoor maar ook daarbuiten werken we veel samen. Let erop dat een collega ook recht op privacy heeft. Soms is het vanuit het vervullen van een functie niet gewenst dat een naam bekend wordt, maar ook op persoonlijk vlak kunnen mensen hier bezwaar tegen hebben. Hou daar rekening mee bij het maken van bijvoorbeeld foto’s of een verslag. Geef dit vooraf aan en vraag naar eventuele bezwaren.

7 Pas op voor cybercriminelen

7.1 Virussen en betrouwbare software

Installeer op je telefoon en tablet alleen maar apps vanuit de officiële appstores (Rijks AppStore, Apple App Store, Google Play, etc.). Apps die van andere plekken komen, kunnen virussen e.d. bevatten. Virussen kunnen documenten heimelijk wijzigen, vergrendelen of zelfs permanent verwijderen waardoor organisaties langdurig niet kunnen werken. Het herstel daarvan is kostbaar. Bovendien loop je hierdoor het risico dat gevoelige informatie via je telefoon uitlekt, zoals je mail en chatberichten, locatie, browser- of contactgegevens.

Installeer op de laptop alleen software rechtstreeks van die ICT-leverancier. Populaire software kan je overal downloaden en ook die bevatten soms virussen. Overleg bij twijfel altijd met je leidinggevende of neem contact op met je IT-dienstverlener.

Op je zakelijke telefoon installeer je alleen apps die je voor het uitvoeren van je functie nodig hebt. Mogelijk bestaat hiervoor een lijst met apps die binnen jouw organisatie worden gebruikt.

Ondanks dat we goed beschermd zijn en ook als je goed oplet, kan het misgaan. Meld dat (zie 2.6).

7.2 Phishing? Tel eerst tot tien!

Laat niet zomaar je gegevens achter.

Cybercriminelen willen graag inloggegevens of financiële gegevens (bv. creditcard) van jou en je organisatie stelen. Dit doen ze onder andere via het zogeheten phishing: via een mailtje, chat/SMS'je, telefoontje of een post op social media, word je bijvoorbeeld "uitgenodigd" je gegevens op een website achter te laten of een bepaalde handeling uit te voeren. Daarna zijn je gegevens in handen van de criminelen en kunnen die misbruikt worden voor bijvoorbeeld identiteitsfraude.

Wat belangrijk is, is dat je eerst even tot tien telt en niet direct op een link klikt, niet direct een bijlage opent en niet directe gegevens via de telefoon weggeeft. Niet ieder mailtje, telefoontje en niet ieder persoon is wat of wie het lijkt te zijn. Zelfs foto's en telefoontjes van 'bekenden' kunnen tegenwoordig 'deepfakes' zijn en dus nep en onbetrouwbaar. Banken en servicedesks vragen in het algemeen niet via de mail om allerlei gevoelige gegevens zoals je wachtwoord.

Twijfel je over de juistheid van een bericht of mailtje overleg dan met collega's en eventueel je servicedesk. Gebruik bij twijfel nooit de contactgegevens uit de mail of bericht, deze zijn mogelijk niet betrouwbaar.

Cybercriminelen vallen met phishingmails ook organisaties aan. Naast phishingmails om je gegevens te stelen gebeurt het ook dat via vergelijkbare technieken virussen worden verspreid, bijvoorbeeld om bestanden op slot te zetten.

Klik dus nooit zomaar op linkjes en bestanden in mailtjes. Als je toch denkt dat het een 'echt' bericht is, klik dan niet op de link, maar ga zelf naar de echte website en log daarin. Of neem zelf rechtstreeks contact op met de echte organisatie per telefoon of mail. Phishing kan grote gevolgen hebben voor de organisatie waarin je werkt maar ook voor

Tooltip: Heb je een phishingmail ontvangen en heeft je organisatie een spam / phishing button? Klik hier op. Dan wordt deze mail in quarantaine gezet en wordt de e-mail verder geanalyseerd door de IT afdeling

jezelf. Dagelijks worden personen en organisaties door dergelijke software aangevallen en het herstel kost veel tijd en geld.

Heb je per ongeluk op een link in een vermoedelijke phishingmail geklikt of een bijlage geopend? Meld dit in ieder geval direct bij je leidinggevende en servicedesk.

7.3 Pas op voor bijzondere en onverwachte berichten

Cybercriminelen proberen je vaak te verrassen waardoor je bijvoorbeeld onder tijdsdruk snel een handeling uitvoert. Bij social engineering en digitale oplichting wordt dit vaak toegepast. Je krijgt dan een bericht (uit naam van) een voor jouw bekende persoon of organisatie met de vraag iets met spoed te doen. Deze berichten kunnen op verschillende manieren binnenkomen, via een mail, SMS- of chatbericht.

Vraagt een bekende plotseling om geld? Bel die persoon!

Cybercriminelen misbruiken je gegevens om geld mee te verdienen. Ze doen zich bijvoorbeeld als jou voor ('social engineering') en vragen je vrienden, familie of collega's om geld, of informatie. 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. Een eerste indruk kan je al krijgen door te bedenken of het logisch is. Een collega zal niet snel een tikkie sturen van 1 cent, terwijl dit voor de criminelen wel een manier is om achter gegevens te komen. Volg dus zeker ook je onderbuikgevoel.

Tooltip: Niet iedereen op internet is wie hij/zij zegt dat hij/zij is. Niet iedereen die hulp aanbiedt, biedt echt hulp aan.

Open geen bijlagen die je niet had verwacht of het nu een grappig filmpje of een zakelijke bijlage lijkt te zijn. Cybercriminelen willen dat je hierop klikt. Deze bijlagen kunnen echter ongewenste inhoud zoals bijvoorbeeld een virus bevatten.

7.4 Gratis software en apps kunnen kostbaar zijn

Maak alleen gebruik van de aangeboden voorzieningen.

Op het internet is veel vrij toegankelijk. Je kan dus gebruik maken van allerlei handige gratis diensten of websites. Ook is er veel software te vinden waarvoor je niet direct hoeft te betalen. 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) en apps of applicaties die je organisatie ter beschikking stelt. Is een dienst of app echt nodig voor de uitvoering je werkzaamheden, neem dan contact op met de servicedesk om te kijken of deze dienst onderdeel kan worden van de standaard dienstverlening. Ook kunnen er regels voor software bestaan die het gebruik hiervan aan banden leggen (licentievoorwaarden).

Geef je gegevens niet zomaar weg voor een gratis app.

Een gratis dienst of app is nooit echt gratis: de aanbieders hiervan 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 of bij het aanmaken van een account toestemming voor gegeven. Die gegevens kunnen ook je contactgegevens en locatiegegevens zijn. Ze weten dan wanneer je waar bent, waar je woont en met wie je in contact bent.

Geef je gegevens of informatie van de overheid niet zomaar weg voor een handige app, maar denk na of het je dat wel waard is.

7.5 Druk, dwang en verleiding: zoek hulp!

Externe partijen kunnen proberen om je dingen te laten doen die niet horen. Ze willen bijvoorbeeld informatie hebben. Je kent ze misschien goed, ze weten mogelijk iets pijnlijks over je of ze proberen je te verleiden met geld. Werk hier niet aan mee. Het kan als iets kleins beginnen maar doe je eenmaal mee, dan is dat meteen weer een nieuw drukmiddel. Als je in een dergelijke situatie gebracht wordt, zoek hulp: je staat er niet alleen voor! Meld dit als incident bij de BVA en je leidinggevende. Neem eventueel ook contact op met een vertrouwenspersoon om de beste stappen te bespreken.

8 Beheer en implementatie

Dit hoofdstuk bevat geen gedragsregels en is vooral bedoeld voor specialisten zoals de CISO's en P&O-adviseurs. Het hoofdstuk beschrijft hoe deze gedragsregeling wordt beheerd en hoe deze bij een organisatie kan worden toegepast.

8.1 Doelgroep

Het doel van deze gedragsregeling is bij te dragen aan de digitale en fysieke weerbaarheid van de Rijksoverheid door het geven van concreet handelingsperspectief voor de goede omgang met de fysieke en digitale werkomgeving en daaraan gerelateerde onderwerpen.

De doelgroep van deze gedragsregeling is niet alleen alle Rijks- en Defensieambtenaren, maar geldt voor alle leidinggevenden en medewerkers die voor de Rijksoverheid werkzaamheden uitvoeren en daarbij gebruik maken 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 aangeduid met (rijks)medewerkers.

8.2 Beheer van het document

Voortdurend komt er nieuwe wet- en regelgeving, zoals enige tijd geleden de Wet Open Overheid (Woo) en de nieuwe Archiefwet. 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:

1. Wijzigingen waarbij hoofdregels, zie deel 1 van het document, veranderen. In dat geval verandert de essentie van de gedragsregeling en is brede afstemming noodzakelijk en hernieuwde instemming van de GOR Rijk. Voor Defensie loopt dit via Centrale medezeggenschapscommissie Defensie;
2. Tekstuele wijzigingen in deel 2 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.

8.3 Uitfaseren andere regelingen en eigen versie van de gedragsregeling

Dit document vervangt alle algemene gedragsregelingen voor de digitale en fysieke werkomgeving. Wel mogen organisaties aanvullende regelingen maken voor de onderwerpen die buiten scope vallen (zie 3.2.1). Eigen algemene regelingen op dit gebied moeten dus uitgefaseerd of te worden samengevoegd met deze regeling in een eigen versie.

Organisaties binnen de Rijksoverheid kunnen indien gewenst een eigen versie van de gedragsregeling digitale werkomgeving uitbrengen. Aanpassingen kunnen op 2 niveaus worden doorgevoerd:

1. In de tekst en bijlagen kunnen organisaties aanvullingen doen voor de eigen specifieke contactpersonen inclusief bereikbaarheidsinformatie, voorzieningen en verwijzingen.
2. Organisaties binnen de rijksoverheid kunnen in samenspraak met hun medezeggenschap ook aanvullende en 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. Indien een organisatie van deze optie gebruik maakt, dient deze aangepaste versie aan de ondernemingsraad te worden voorgelegd.

Als een organisatie een eigen versie maakt, dient de naam van de organisatie te worden in de titel op de voorpagina worden opgenomen en de tekst 'Algemene rijksbrede versie' vervangen. De eigen regeling moet ook voldoen aan de toegankelijkheidscriteria (zie 8.4).

8.4 Toegankelijkheid

Bij de opstelling en vormgeving van het document is veel aandacht besteed aan de toegankelijkheid.

Taalgebruik; het taalgebruik dient aan te sluiten op het niveau B1. Hierdoor is het document toegankelijk voor de hele doelgroep. Deze versie van de gedragsregeling is op verschillende manieren getoetst tegen het B1-niveau.

Toegankelijkheid voor medewerkers met een (visuele) beperking. Bij de opmaak van het document is rekening gehouden met de eisen voor digitale toegankelijkheid zodat het document in zijn geheel toegankelijk is voor medewerkers met bijvoorbeeld een visuele beperking, eventueel met gebruik van hulpmiddelen.

Bij aanpassingen en vernieuwingen wordt dit gehandhaafd.

8.5 Rollen, taken en bevoegdheden

Algemene verantwoordelijkheden.

Voor het volgen van de gedragsregeling gelden de volgende algemene verantwoordelijkheden

8.5.1 Medewerker – eigen verantwoordelijkheid

Zoals hiervoor aangegeven is de medewerker zelf verantwoordelijk voor eigen gedrag en keuzes. Hij moet de gedragsregels toepassen en raadpleegt deze wanneer nodig.

8.5.2 Leidinggevende – voorbeeldgedrag, stimuleren en sturen

De leidinggevende heeft een belangrijke rol: hij vertoont voorbeeldgedrag, hij stimuleert de: medewerkers om de regels te volgen, biedt opleidingen aan, stuurt op het volgen en toepassen van programma's en instrumenten die door P&O en de CISO worden aangeboden en spreekt medewerkers aan die de regels niet volgen. Hij stimuleert een cultuur waarin ieder elkaar helpt en om hulp vraagt en waarin, fouten melden en bespreken normaal is en veilig kan.

Specifieke verantwoordelijkheden

Voor de implementatie van de gedragsregeling, gelden de volgende specifieke verantwoordelijkheden.

8.5.3 CIO Rijk

CIO Rijk is verantwoordelijk voor het opstellen, actueel houden en bekendmaken van de gedragsregeling. Daarnaast monitort en faciliteert CIO Rijk de implementatie.

8.5.4 *CIO Departement*

De departementale CIO heeft een overkoepelende verantwoordelijkheid voor de departementale implementatie van de gedragsregeling in de samenwerking tussen HR-adviseur en de CISO

8.5.5 *CISO Departement*

De CISO organiseert namens de CIO van specifieke programma's en activiteiten gericht op bewustwording en gedragsverandering in lijn met de gedragsregeling.

8.5.6 *P&O-adviseur*

De P&O-adviseur biedt algemene voorzieningen en ondersteuning voor leidinggevenden en medewerkers voor de uitvoering van de gedragsregeling

Wat	A	R	C	I
Opstellen en bekendmaken gedragsregeling + monitoren en faciliteren implementatie	CIO-Rijk	CISO-Rijk	BVA – beraad CISO – raad CIO – beraad CPO – raad GOR-Rijk ICBR ICOP	Alle medewerkers
Beoordelen noodzaak eigen versie van de gedragsregeling en evt. opstellen	CIO	CISO	P&O Mede-zeggenschap	Algemeen Directeur
Departementaal bekendmaken van de gedragsregeling	CIO	CISO	P&O adviseur BVA	Alle medewerkers
Monitoren en controleren van het informatie-beveiligings-bewustzijn	CIO	CISO [2]	P&O adviseur	Algemeen Directeur CIO-Rijk CISO-Rijk

Tabel 1: RACI-tabel gedragsregeling

Toelichting: De letters van het RACI model staan voor rollen:

R – Responsible (Verantwoordelijk): Degene die verantwoordelijk is voor de uitvoering. Verantwoording wordt afgelegd aan de persoon die accountable is.
A – Accountable (Eindverantwoordelijk): Degene die (eind)verantwoordelijk, bevoegd is en goedkeuring geeft aan het resultaat.
C – Consulted (Geraadpleegd): Deze persoon geeft (mede) richting aan het resultaat, hij/zij wordt voorafgaand aan beslissingen of acties (verplicht) geraadpleegd.
I – Informed (Geïnformeerd): Wordt geïnformeerd over beslissingen, voortgang en bereikte resultaten.

[2] Conform: Besluit CIO-stelsel Rijksdienst 2021 | Besluit | Rijksoverheid.nl

Bijlage 1 – Veilige voorzieningen

Rijksbrede voorzieningen

Voorziening	Rubricering	Bijzonderheden
Samenwerkruimten(SWF)	DepV/BBN2	
Mail	DepV/BBN2, mits binnen rijksoverheid, zie 4.1	
Harde schijf encryptie/ Safeguard*	DepV	
Mobiele telefoon/tablet: Blackberry Work-apps Mobile Iron-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 WOO

- Afdeling communicatie: <mailadres, telefoonnummer>
- Coördinator Woo: <naam, mailadres, telefoonnummer>
- Woo-jurist: <naam, mailadres, telefoonnummer>

Bijlage 3 – Verwijzingen naar achterliggende documenten

1. Gedragscode Integriteit Rijk: Gedragscode Integriteit Rijk | Richtlijn | Rijksoverheid.nl

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

3. Integriteitsschendingen en Baseline Intern persoonsgericht onderzoek na een integriteits- of beveiligingsincident (BIPO): https://rijksportaal.overheid-i.nl/onderwerpen/personeel/artikelen/rechten-en-regels/integriteit/integriteitsschendingen.html

4. Handreiking Online Communicatie Rijksambtenaren: Handreiking online communicatie rijksambtenaren | Rapport | Rijksoverheid.nl

5. Website open op orde: Open op Orde | Over Open Overheid | Open Overheid (open-overheid.nl)
   Kenniskaart werken met informatie, Kenniskaart werken met informatie: waarom is belangrijk en wat willen we bereiken: https://www.informatiehuishouding.nl/documenten/instrumenten/2019/09/17/kenniskaart-werken-met-overheidsinformatie

6. Instructie voor openbaar maken: https://www.informatiehuishouding.nl/documenten/publicaties/2024/10/22/handreiking-openbaar-maken-doe-je-zo---conceptversie

7. Rijkshuisstijl: https://rijksportaal.overheid-i.nl/onderwerpen/communicatie/huisstijl-en-vormgeving

8. Beeldbankfotografie: https://rijksportaal.overheid-i.nl/onderwerpen/communicatie/artikelen/huisstijl-en-vormgeving/beeld-en-vormgeving/welke_beeldbanken_kun_je_gzebruiken_.html

9. Instructie wachtwoorden: https://rijksportaal.overheid-i.nl/onderwerpen/werkplek/artikelen/online-veiligheid/wachtwoorden/wachtwoorden.html

10. Instructie Keepass (SSC-ICT): https://topdesk-sscict.rijksweb.nl/tas/public/ssp/content/detail/knowledgeitem?unid=3e2ee344%2Dacec%2D4187%2D8576%2Db6b9a68b5fc8

11. Instructie flex2rijk (SSC-ICT): https://topdesk-sscict.rijksweb.nl/tas/public/ssp/content/detail/knowledgeitem?unid=5e88789cd0ea411c9861f427427bbce4

12. Instructie voor samenwerkruimten: https://rijksportaal.overheid-i.nl/onderwerpen/werkplek/artikelen/ict/applicaties/samenwerkruimten.html

13. instructie 7Zip; op te vragen bij de ICT-servicedesk

14. Instructie SecureTransfer: https://securetransfer.rijkscloud.nl/static/securedropzone/handleiding.pdf

15. Instructie bestandenpostbus: Bestandenpostbus (overheid-i.nl)

16. Handreiking m.b.t. berichtenapps:
https://www.informatiehuishouding.nl/Producten+%26+publicaties/richtlijnen/2018/02/07/beleidslijn-berichtenapps
https://www.informatiehuishouding.nl/leerhuis-en-campagnes/app-met-beleid

17. Handreiking opslaan chatberichten:
https://www.informatiehuishouding.nl/documenten/rapporten/2022/08/01/handreiking-bewaren-chatberichten

18. Instructies voor Webex: https://services.belastingdienst.nl/rijksvideodienst/
Best Practices For Working Remotely (webex.com)
Helpcentrum van Webex

19. Fiscaal vriendelijke doelen IKB: Fiscaalvriendelijke doelen | Personele informatie Rijk | O&P Rijk P-Direkt

20. Aanvragen WIFI:
Wifi - Rijksportaal (overheid-i.nl)

21. Gebruik hotspot: Instructie voor instellen telefoon als hotspot bij 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

22. Landen die deel uitmaken van de Europese Economische Ruimte (EER).
https://www.rijksoverheid.nl/onderwerpen/europese-unie/vraag-en-antwoord/welke-landen-horen-bij-de-europese-economische-ruimte-eer

Bijlage 4 – Verklarende woordenlijst

Archivering
Archiveren is het duurzaam toegankelijk maken en houden van informatie Hierdoor is de informatie nu en in de toekomst bruikbaar. Iedereen die het recht heeft om de informatie in te zien moet er ook in de toekomst nog toegang tot hebben.

Autoriteit Persoonsgegevens (AP)
De AP is de Nederlandse toezichthouder voor het toezicht op het verwerken van persoonsgegevens. De organisatie houdt zich dus bezig met privacy. De taken van de AP vloeien voort uit de Europese Algemene verordening gegevensbescherming (AVG).

AVG-verzoeken
Verzoeken van personen (betrokkenen) onder de Algemene Verordening Gegevensbescherming (AVG) voor inzage in, correctie van, of verwijdering van hun persoonsgegevens.

Beeldbanken
Databases of archieven die afbeeldingen of visuele media bevatten, vaak gebruikt voor communicatie, ontwerp of educatieve doeleinden.

Briefgeheim
In de wet vastgelegde garantie dat de tekst in een brief niet zomaar mag worden ingezien.

BVA
Bij ieder departement is een Beveiligingsautoriteit (BVA) werkzaam. De BVA draagt zorg voor het toezicht op de integrale beveiliging van het departement en de organisatie hiervan. Een BVA adviseert, ondersteunt, houdt toezicht en onderzoekt incidenten op het gebied van integrale beveiliging. Daaronder valt beveiliging van informatie, personeel, materieel en gebouwen. Maar ook het creëren van bewustwording van risico’s en maatregelen valt binnen het werkveld van een BVA.

CISO
Chief Information Security Officer, de persoon binnen een organisatie die verantwoordelijk is voor het ontwikkelen en implementeren en naleving van het informatiebeveiligingsbeleid**.**

Cloudapplicatie
Softwaretoepassingen die worden gehost en geleverd door een serviceprovider, vaak via het internet, waardoor gebruikers toegang hebben tot gegevens en functionaliteit vanaf verschillende apparaten en locaties**.**

CPO
Chief Privacy Officer, de persoon binnen een organisatie die verantwoordelijk is voor het beheer en de naleving van privacyregelgeving en -beleid.

Cybercriminaliteit
Activiteiten waarbij smartphones, computers en netwerken worden gebruikt of aangevallen om misdaden te plegen, zoals hacken, verspreiden virussen en cyberaanvallen e.d.

Datalek
Een beveiligingsincident waarbij persoonsgegevens geraakt worden. Bijvoorbeeld doordat personen toegang hebben tot persoonsgegevens zonder dat dat de bedoeling is of dat ze dat mogen. Maar ook het per ongeluk vernietigen van persoonsgegevens, of doorsturen van persoonsgegevens.

Dataminimalisatie
Het bewust beperken van het verzamelen en het gebruiken van persoonsgegevens tot wat absoluut moet om een specifiek doel te bereiken. Niet meer gegevens gebruiken dan strikt noodzakelijk.

Handelingsperspectief
Alle zaken die je tot je beschikking hebt om een actie te ondernemen of beslissingen te nemen. Denk hier aan het gebruiken van beschikbare informatie en middelen.

Informatiebeveiligingsincident
Een gebeurtenis die de vertrouwelijkheid, integriteit of beschikbaarheid van informatie in gevaar brengt. Denk aan vertrouwelijke informatie (bijvoorbeeld wachtwoorden of documenten) die in verkeerde handen komt. Of dat iemand toegang krijgt tot een systeem waar dat niet de bedoeling is

Intellectueel eigendom
Rechten op uitgewerkte ideeën, teksten, muziek, foto's, uitvindingen e.d. Deze rechten beschermen de eigenaar tegen het niet goedgekeurde gebruik van zijn werk.

Onbevoegden
Personen die geen toestemming hebben om toegang te krijgen tot bepaalde informatie, systemen of locaties. Bijvoorbeeld inbrekers, maar ook collega’s die de toestemming niet hebben.

Persoonsgegevens
Informatie die direct of indirect iets zegt over een mens (herleidbaar is). Persoonsgegevens kunnen worden gebruikt om een persoon aan te wijzen door bijvoorbeeld een naam, adres, e-mailadres, maar ook alle andere informatie die iets zegt over een persoon.

Phishing
Een vorm van cyberaanval waarbij criminelen proberen informatie te achterhalen door zich voor te doen als een betrouwbare organisatie of persoon via e-mail, websites, berichten of telefoongesprekken.

Servicedesk
Een afdeling of team binnen een organisatie die helpt bij het zorgen voor een oplossing voor problemen met ICT-middelen en systemen. Ook wel bekend als helpdesk.

Social Engineering
Het misbruiken van dingen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Criminelen proberen zo vertrouwelijke informatie van iemand los te krijgen, of toegang te krijgen tot een systeem of gebouw. Ze willen bijvoorbeeld persoonlijke gegevens en beveiligingscodes te weten komen of kwaadaardige software installeren.

Software
Programma's en applicaties (apps) die op computers, smartphones en andere

apparaten worden uitgevoerd om specifieke taken uit te voeren of functionaliteit te bieden.

Woo-verzoek
Een verzoek aan een overheidsinstantie om informatie te verstrekken op basis van de Nederlandse Wet open overheid. Een Woo-verzoek kan betrekking hebben op verschillende soorten informatie, zoals documenten, rapporten, notulen van vergaderingen, of andere gegevens die onder de verantwoordelijkheid van de overheidsinstantie vallen.

Het is altijd mogelijk dat je term tegen komt die nieuw voor je is. Dan is het Cybersecuritywoordenboek een handig hulpmiddel om dit op te zoeken. Dit woordenboek kun je vinden op https://cyberveilignederland.nl/woordenboek