COA Centraal Orgaan opvang asielzoekers

COA-Gedragsregeling

voor de digitale werkomgeving

datum:	20-01-2022
naam:	CISO en Beleidsadviseur Arbeidsvoorwaarden
bedrijfsonderdeel:	Informatiebeveiliging en HR&O
versie:	Definitief 1.1

COA Centraal Orgaan opvang asielzoekers

Voorwoord

Deze gedragsregeling maakt onderdeel uit van de Gedragscode integriteit en vormt samen met het 'Beleid alcohol, drugs en medicijnengebruik door COA medewerkers' en de 'COA-Gedragsrichtlijnen Sociale Media' het tweede deel van de gedragscode.
Deze gedragsregeling is in basis gelijk aan de binnen het Rijk geldende variant, maar passend voor de specifieke COA-organisatie gemaakt. Het verplicht volgen van de basiscursus risicobewust handelen 'hoe alert ben jij' is toegevoegd. Dit geldt voor alle organisaties vallend onder het Ministerie van Veiligheid en Justitie.

Nieuwe medewerkers ontvangen dit document voor indiensttreding en gaan met het tekenen van de arbeidsovereenkomst akkoord met de inhoud daarvan.

Contactpersonen (functies) met betrekking tot de Gedragsregeling voor de digitale werkomgeving:

- Informatiebeveiliging: CISO
- HR&O: Beleidsadviseur Arbeidsvoorwaarden

COA Centraal Orgaan opvang asielzoekers

Inhoud

COA Centraal Orgaan opvang asielzoekers

1. Gedragsregeling voor de digitale werkomgeving

1.1 Inleiding

Als medewerker krijg je de beschikking over een fysieke werkplek met een vaste computer en/of een laptop en een 'digitale werkomgeving' (inlogaccount). Mogelijk heb je ook nog een smartphone of tablet van het COA.

Op de vaste computer of laptop wordt een volledige digitale werkomgeving beschikbaar gesteld aan alle medewerkers van het COA. Op de andere mobiele middelen worden beperkte functionaliteiten, zoals alleen vergader-, agenda-en e-mailvoorzieningen verstrekt. Jouw functie en het soort informatie waarmee jij werkt, is bepalend voor welke ICT-functionaliteiten nodig zijn voor jouw functie-uitoefening. Dit wordt door je leidinggevende vastgesteld. Die bepaalt welke ICT-mogelijkheden, zoals een smartphone, tablet of andere mobiele middelen beschikbaar gesteld kunnen worden.

Als je met een tablet of smartphone werkt, kun je e-mail ontvangen en op toegestane apps kun je een deel van je werkzaamheden verrichten. Dit is daarom geen volledige digitale werkomgeving. In deze Gedragsregeling wordt soms onderscheid gemaakt tussen de volledige digitale werkomgeving en voorzieningen met beperkte toegang tot de digitale werkomgeving.

De digitale werkomgeving biedt jou mogelijkheden die een zeker risicobesef vragen. Deze Gedragsregeling voor de digitale werkomgeving bevat daarom afspraken over de gebruiksmogelijkheden van de digitale werkomgeving, jouw online gedrag en bewuste omgang met de risico's.

Het is van belang dat je je bewust bent van bestaande wettelijke rechten en plichten en van de mogelijke risico's. Dat stelt jou in staat om je eigen verantwoordelijkheid te kunnen nemen. Daarom heeft het COA bestuur naast de technische beveiliging en voorzieningen voor het vergroten van de weerbaarheid van het COA als organisatie en ter vermijding van eventuele risico's deze Gedragsregeling voor de digitale werkomgeving[1] opgesteld. Deze Gedragsregeling is een uitwerking van goed ambtenaarschap en wat de maatschappij mag verwachten van een COA-medewerker[2].

[1] Op grond van het koninklijk besluit van 18 oktober 1988, houdende regeling van de functie en verantwoordelijkheid van de secretaris-generaal, alsmede het Voorschrift Informatiebeveiliging Rijksdienst (2013) https://wetten.overheid.nl/BWBR0033507/2013-06-01

[2] Ambtenarenwet 2017, artikel 6 regelt dat iedere ambtenaar zich als een goed ambtenaar behoort te gedragen.

Je hoort je hieraan te houden en bent hierop aanspreekbaar. In eerste instantie zal je leidinggevende[3] toezien op de naleving hiervan. De beveiligingtoezichthouders[4] houden namens het bestuur in tweede instantie het toezicht op naleving. Niet naleving van deze regels kan leiden tot maatregelen.

Deze Gedragsregeling beschrijft concreet het van jou gewenste gedrag bij het gebruik van de digitale werkomgeving, geeft een algemene toelichting daarop en geeft je nadere informatie over het beheer van en de controle op de digitale werkomgeving.

1.2 Een betrouwbare en weerbare informatievoorziening

Het COA waarborgt met back-ups en technische beveiligingsmaatregelen de beschikbaarheid, duurzame toegankelijkheid, integriteit en vertrouwelijkheid van de informatie. In hoofdstuk 3 worden de technische voorzieningen en procedures toegelicht die het COA ingericht heeft. Niet alle risico's zijn echter technisch te ondervangen, waardoor afspraken over gebruiksmogelijkheden van digitale werkomgevingen en online gedrag nodig zijn. Veilig, effectief en efficiënt gebruik van digitale werkomgevingen draagt bij aan de betrouwbaarheid en weerbaarheid[5] van de informatievoorziening.

Met het naleven van deze Gedragsregeling draag je bij aan de betrouwbaarheid en weerbaarheid van de informatievoorziening van het COA.

1.3 Professioneel en integer online gedrag

Van alle medewerkers wordt professioneel en integer handelen verwacht.

Het bezoeken van sites, downloaden of verzenden van informatie met een pornografische, racistische, discriminerende, extremistische, terroristische, aanstootgevende of – al dan niet seksueel -intimiderende of anderszins beledigende of bedreigende inhoud, is niet toegestaan. Uitzondering hierop vormt de uitoefening van opgedragen werkzaamheden[6].

[3] Beveiligingsvoorschrift Rijksdienst 2013, artikel 4 lid 3. https://wetten.overheid.nl/BWBR0033512/2013-06-01

[4] Beveiligingstoezichthouders: COA kent geen BVA. Binnen COA zijn de CISO, Privacy Officer, adviseur Veiligheid en adviseur Integriteit gezamenlijk belast met de integrale beveiliging van organisatie, medewerkers, materieel, informatiesystemen, gebouwen en overige objecten, alsmede het toezicht op de werking van de beveiligingsorganisatie en de informatiebeveiliging.

[5] Weerbaarheid van de informatievoorziening is het vermogen van de digitale werkomgeving om weerstand te bieden tegen voorstelbare dreigingen.

[6] Voor specifieke opgedragen werkzaamheden is het mogelijk dat voorafgaande een ontheffing wordt gegeven. Dat zal doorgaans voortvloeien uit onderzoek waarvoor een juridisch toets heeft plaatsgevonden en noodzakelijkheid is gebleken.

1.4 Zorgvuldig gebruik van de voorzieningen

Bij vermissing of het vermoeden van diefstal van (onderdelen van) digitale mobiele apparatuur en gegevensdragers van het werk, meld je dit direct bij je direct leidinggevende. Ook doe je bij het vermoeden van diefstal aangifte bij de politie en verstrekt een kopie van het proces-verbaal aan de medewerker van ICT die de nieuwe apparatuur uitlevert.

Laat mobiele apparaten en gegevensdragers (laptop, smartphone, tablet, usb-stick) nooit ergens liggen, zonder dat je vastgesteld hebt dat het voor onbevoegden onmogelijk is om toegang tot de informatie te krijgen.

Je bent zelf verantwoordelijk voor de handelingen die jij verricht dan wel laat verrichten onder jouw persoonlijke toegang (inloggegevens) tot de Digitale werkomgeving en op de apparatuur die je van je werk hebt ontvangen. Deze leen je dus niet uit aan anderen, ook niet aan je kinderen. Je installeert bijvoorbeeld geen Tor-browser[7] op apparatuur van je werk. Ook bezoek je geen geblokkeerde websites.

Je kunt op die verantwoordelijkheid worden aangesproken door je leidinggevende en door de beveiligingstoezichthouders. Inbreuk op de Gedragsregeling wordt beschouwd als plichtsverzuim. Dit kan verschillende sancties tot gevolg hebben, afhankelijk van de aard en ernst van het vastgestelde plichtsverzuim.

1.5 Schade, dat kan gebeuren

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

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

Vertrouw je het bericht niet, open de e-mail dan niet verder. Meld dit bij de ICT-servicedesk en volg hun aanwijzingen op. Klik nooit op verdachte bijlagen, links, pop-ups en banners. Die bevatten vaak virussen en malafide software.
Schade kan ook ontstaan door software te installeren op de computers en laptops of door vanaf een mobiele gegevensdrager (usb-stick, externe harde schijf, etc.) software te draaien op deze digitale werkomgevingen. De ICT-beheerorganisatie heeft de mogelijkheid om dergelijke software te blokkeren.

[7] TOR: The Onion Router, een speciaal netwerk dat gebruikers anonimiseert.

Wanneer de betreffende functionaliteiten noodzakelijk zijn voor het werk, dan kan in overleg met en met toestemming van de leidinggevende een verzoek aan de ICT-beheerorganisatie gericht worden via de ICT-servicedesk.

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

1.6 Meld incidenten en kwetsbaarheden

Jij bent medeverantwoordelijk voor de betrouwbaarheid en weerbaarheid van de informatievoorziening van het COA. Daarom wordt van jou veilig en integer handelen verwacht. Daarbij hoort ook dat je alert bent en zaken signaleert. Wanneer je iets afwijkends opmerkt of iets niet vertrouwt, help je mee door dit zo snel mogelijk (in ieder geval binnen 24 uur na bekendwording) te melden als incident:

a. Technische incidenten (bijvoorbeeld een virus): meld dit bij de ICT-servicedesk.
b. Een kwetsbaarheid in de digitale werkomgeving: meld dit bij je direct leidinggevende en de ICT-servicedesk. Deze informatie behandel je als departementaal vertrouwelijk (Dep.V.)[8].
c. Overige incidenten (bijvoorbeeld diefstal of verlies): als vertrouwelijke informatie (mogelijk) in handen is gekomen van onbevoegden, meld dit direct bij je leidinggevende en de ICT-servicedesk.
d. Inhoud van een bericht (bijvoorbeeld aanstootgevende inhoud of mogelijke phishing): Informeer je leidinggevende en vraag advies aan de ICT-servicedesk als je de inhoud van een bericht of de werking van een programma niet vertrouwt. Als het vermoeden bestaat, dat deze inhoud opgeslagen is op de infrastructuur van het COA, zal deze digitale werkomgeving onmiddellijk worden afgesloten. Meld dit dan aan je leidinggevende, zodat je je werkzaamheden op een andere manier kunt voortzetten.
e. Ongewenst omgangsvormen zoals in de Gedragscode Integriteit COA is omschreven, kun je melden bij je leidinggevende of bij een vertrouwenspersoon[9]. Indien er sprake is van een (vermoeden van een) integriteitschending moet dit worden gemeld bij en geregistreerd door het meldpunt Integriteit of de adviseur Integriteit[10].

1.7 Persoonlijk gebruik is toegestaan

Als medewerker ben je zelf verantwoordelijk en aanspreekbaar voor de zorgvuldige omgang met (waaronder de beveiliging en opslag van) je werkbestanden.
Op de computer of de laptop die door het COA beschikbaar wordt gesteld is een beveiligde, werk gerelateerde omgeving ingesteld.

Beperkt privégebruik van de digitale werkomgeving is toegestaan, mits dit niet storend is voor de dagelijkse werkzaamheden of extra belastend voor het computernetwerk.

[8] Departementaal Vertrouwelijk (afgekort Dep.V.) : Indien kennisname door niet geautoriseerden schade kan toebrengen aan de belangen van één of meerdere ministeries.
[9] Vertrouwenspersonen COA: https://plein-intranet.coa.local/HRO/geni/Paginas/Vertrouwenspersonen.aspx
[10] Melden van integriteitschendingen: https://plein-intranet.coa.local/HRO/geni/Paginas/Meldpunt-integriteit.aspx

Om de privacy te waarborgen, is het van belang dat jij jouw privébestanden, -berichten en dergelijke duidelijk van werkgerelateerde informatie gescheiden houdt. Dit doe je door ze apart in mappen met 'Privé' in de naam op te slaan.

Het COA zal het privékarakter van digitale persoonlijke bestanden van medewerkers respecteren en mag niet zonder meer toegang krijgen daartoe. In bijzondere omstandigheden kan de werkgever toegang aanvragen (zie: Toegang i.v.m. continuïteit van werkzaamheden[11]).

Het automatisch doorsturen van berichten die binnenkomen op je werk e-mail account, naar een privé e-mail adres is niet toegestaan. Je kunt dan immers niet controleren of er vertrouwelijke informatie tussen zit.

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

Ga verstandig om met het gebruik van je werk e-mailadres voor privéactiviteiten. Denk hierbij ook aan het aanmelden voor nieuwsbrieven en het reageren op reclame. Zo draag je bij aan het voorkomen van spam. Ook het gebruik van sociale media en het afspelen van films en muziek vragen veel capaciteit van mobiele apparaten, zoals je telefoon en tablet. Onbedoeld kun je door je gedrag het COA op kosten jagen, die bijvoorbeeld via je telefoonabonnement lopen. Met name in het buitenland verbruik je snel veel data, tegen hoge kosten. Beperk daarom in het buitenland het privégebruik van apparatuur van je werk.

Financiële transacties voor privédoeleinden op kosten van het COA zijn niet toegestaan op of via de digitale werkomgeving[12]. Dit omvat commerciële activiteiten, zoals bestellingen en boekingen, beurshandel, gokken of spelletjes met financiële verrekening of betaalde telefoondiensten.

Behalve dat via dergelijke interacties virussen en malafide software op de voorzieningen van het COA terecht kunnen komen, kunnen kwaadwillenden zo naast ongeautoriseerde toegang tot de netwerken van het COA ook makkelijker jouw financiële en privé gegevens verkrijgen. Bovendien kan het schadelijk zijn voor het imago van het COA.

Een uitzondering is internet bankieren via een beveiligde verbinding met je bank. Controleer of de verbinding beveiligd is door het slotje in de adresbalk.

[11] Procedure 'Verlenen tijdelijk toegang tot e-mailboxen van medewerkers' van de ICT-Servicedesk.
[12] Financiële transacties voor privédoeleinden op eigen kosten via apps op COA smartphones en tablet zijn toegestaan onder eigen verantwoordelijkheid.

Besef dat, bij het gebruik van de digitale werkomgeving voor privédoeleinden, al jouw activiteiten via een digitale werkomgeving op het internet door vele partijen kunnen worden vastgelegd en meegelezen.

Via de digitale werkomgeving ben je op internet herkenbaar als medewerker van het COA.

In je mailadres staat de organisatie waar jij werkt. Het IP-adres[13] waar jouw computer of laptop gebruik van maakt, is een uniek nummer waarmee je op het internet zichtbaar bent als COA-medewerker. Dit is door kwaadwillenden te achterhalen. Via jouw online gedrag, ook als privépersoon, kunnen kwaadwillenden door combinatie van informatie een profiel opmaken, waaruit af te leiden valt hoe interessant jouw werk en jouw informatie is.

De richtlijnen over hoe overheden moeten handelen bij ontvangst, beantwoording en archivering van e-mail zijn te vinden onder: https://www.overheid.nl/contact/e-mailgedragslijn-voor-overheden

[13] Iedere computer die verbonden is met Internet gebruikt een eigen nummer, een IP-adres (IP staat voor "Internet Protocol"). Dit IP-adres kun je zien als het telefoonnummer van de computer. Computers gebruiken IP-adressen om onderling gegevens uit te wisselen.

1.8 Online samenwerken

Het COA biedt met de Digitale werkomgeving veilige mogelijkheden voor online samenwerken met collega's van andere departementen en met externen. Er zijn samenwerkingsfunctionaliteiten voor het delen en opslaan van bestanden en samenwerken tussen de kerndepartementen en uitvoeringsorganisaties en met externen[14]. Ook wordt het aanbod aan voorzieningen die tijd-, plaats-en apparaatonafhankelijk werken verder ondersteunen nog verder uitgebreid.

Bedenk bij het delen van informatie telkens of er schade kan ontstaan wanneer de informatie in handen komt van andere mensen dan voor wie de informatie bedoeld is. (politieke, financiële, imago, juridische, etc schade).

Het aanbod van openbare apps en online voorzieningen is groot. Gebruik die openbare voorzieningen alleen voor openbare informatie. Er kleven aan deze openbare voorzieningen ernstige bezwaren, zoals risico's op het gebied van het eigenaarschap van de informatie, de beschikbaarheid, juistheid en volledigheid en de beveiliging en vertrouwelijkheid van de informatie. Zie ook Apps op een tablet of smartphone.

Moet je jouw gegevens invullen, bijvoorbeeld voor het aanmelden voor een werkgerelateerde congres of cursus, check dan of de link verwijst naar een pagina die begint met https en een slotje in de adresbalk heeft. Dan is het een veilige pagina.

Vertrouwelijke informatie mag niet opgeslagen of gedeeld worden via een samenwerkomgeving of opslagruimte die niet door het Rijk aangeboden wordt.

Sla vertrouwelijke, gerubriceerde[15] of privacygevoelige gegevens nooit in deze openbare online diensten op.

Voor jouw omgang met social media en je gedrag in de Samenwerkingsfunctionaliteit gelden de uitgangspunten uit de COA Sociale Media Richtlijnen[16].

Wees altijd zorgvuldig, betrouwbaar, integer en respectvol in je uitlatingen.

[14] Samenwerkingsfunctionaliteiten op Rijksportaal: http://portal.rp.rijksweb.nl/irj/portal/anonymous/facilitair/ict_en_informatievoorziening%20enhttp://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4/cissamenwerkruimten&NavigationContext=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/cissamenwerkfunctionaliteit_4

[15] Rubricering van gegevens behelst het toekennen van een standaard risicoclassificatie aan informatie. Op basis van de rubricering kunnen de noodzakelijke beveiligingsmaatregelen worden bepaald.

[16] Social Media Richtlijnen COA: https://plein-intranet.coa.local/HRO/geni/Paginas/Social-media-richtlijnen.aspx

1.9 Tijd-, plaats-en apparaatonafhankelijk werken (TPAW) kan

Je leidinggevende bepaalt welke voorzieningen jij nodig hebt voor je werk. In overleg en met toestemming kan je leidinggevende jou, naast de vaste computer of laptop, een digitale werkomgeving op een tablet (via goedgekeurde applicaties) of in de vorm van een telewerkomgeving beschikbaar (via een beveiligde telecommunicatieverbindingen) beschikbaar stellen. Op de smartphone of tablet die je van je werk hebt gekregen, kun je mail ontvangen en versturen via goedgekeurde applicaties. Zo kun je tijd-en plaatsonafhankelijk werken.

Meer informatie over tijd en plaatsonafhankelijk werken vind je op de Plein-pagina over werken @COA[17].

De afspraken over waar jouw eigen voorzieningen aan moeten voldoen en over het gebruik van die tablets en telewerkvoorzieningen, worden vastgelegd in een overeenkomst. Het gebruiken van eigen media voor dataopslag is niet toegestaan.

1.10 Werkbezoek aan het buitenland

Heb je tijdens een werkbezoek aan het buitenland je laptop, mobiele telefoon of tablet die door je werk is verstrekt nodig? Het kan zijn dat contact via buitenlandse providers of online toegang afgeschermd is. Als je naar een hoog-risicoland gaat, is het niet toegestaan om je reguliere laptop, mobiele telefoon of tablet mee te nemen. Voor een werkbezoek aan hoog risicolanden, dienen apparaten gebruikt te worden die specifiek geschikt zijn voor het gebruik in die landen. Vraag dan aan je leidinggevende, team Uitvoering Buitenland of beveiligingstoezichthouders welke aanvullende regels van toepassing zijn voor jouw organisatie. Raadpleeg ook de richtlijn “Werken in het buitenland”.

Neem bij vragen contact op met de ICT servicedesk.

1.11 Mobiel veilig werken

Het werken met mobiele apparaten, zoals de laptop, smartphone of tablet van je werk of via een Telewerkomgeving, is beveiligd. Bij het inloggen op je account wordt een beveiligde verbinding gemaakt. Hiermee wordt de toegang tot het werkgerelateerde deel op het mobiele apparaat gescheiden van het openbare deel waar je bijvoorbeeld privé sociale media apps op kunt installeren en gebruiken. Kwaadwillenden kunnen zo niet via een app bij jouw werkgerelateerde informatie.

Wees echter alert op het openen van bijlagen en documenten, die je op de laptop, smartphone of tablet van je werk of (eigen) computer ontvangt.

Schakel bluetooth, roaming, GPS en persoonlijke hotspot standaard uit en schakel het pas in als je het echt nodig hebt. Anders wordt de smartphone of tablet van je werk onnodig extra kwetsbaar.

[17] Werken @COA: https://plein.coa.local/leesactueel/AtCOA/Paginas/default.aspx

Gebruik het alleen wanneer je het echt nodig hebt, het noodzakelijk is voor je werk en alleen wanneer je in een veilige omgeving kan werken.

Voor meer informatie kun je contact opnemen met de ICT servicedesk.

1.12 Werken met je eigen apparatuur

Indien je met toestemming van de leidinggevende met je eigen smartphone of tablet mag werken en daarvoor toegang tot werkmail- en agendafunctionaliteit op je eigen smartphone of tablet krijgt, wordt er een app toegevoegd die een beveiligde verbinding maakt naar die werkgerelateerde informatie. Zo ontstaat er een werkgerelateerd deel en een openbaar deel.

Op je eigen smartphone en -tablet mag je geen vertrouwelijke of privacygevoelige documenten downloaden naar, opslaan en bewerken in het openbare gedeelte van het apparaat.

Zorg ervoor dat jouw werkgerelateerde informatie alleen op de centrale digitale werkomgeving opgeslagen is.

Het werkgerelateerde deel wordt door de ICT-beheerorganisatie beveiligd en (op afstand) gemanaged. Bij schade, verlies en diefstal zal de ICT-beheerorganisatie de informatie van je digitale werkomgeving, tablet of smartphone op afstand verwijderen.

Zorg voor optimale beveiliging van je eigen computer en mobiele apparaten waarop jij werk gerelateerde informatie verzendt of ontvangt.

Als medewerker blijft je zelf verantwoordelijk voor aanschaf, onderhoud, verzekering en gebruik, wanneer je eigen apparatuur en software inzet voor werk gerelateerd gebruik.

Behalve voor die beveiligde werkomgeving en verbinding, ben je zelf verantwoordelijk voor de benodigde technische inrichting van de informatiebeveiliging op jouw apparatuur en software. De afspraken dienen te worden vastgelegd in een gebruikersovereenkomst.

Laat vóór reparatie of verkoop altijd eerst de werkgerelateerde gegevens en apps van het apparaat wissen bij de ICT servicedesk.

Voor meer informatie kun je contact opnemen met de servicedesk van de ICT-beheerorganisatie.

1.13 Apps op een tablet of smartphone

Op je tablet of smartphone is het toegestaan om apps uit de normale app-stores te downloaden. Let op dat sommige apps gebruik maken van in-app aankopen, die ongemerkt tot hoge kosten kunnen leiden. De kosten voor het aanschaffen en gebruiken van de apps zijn voor eigen rekening.

Wees je bewust van de rechten die een app vraagt en ga hier verstandig mee om. Stel zelf de rechten in.

Sommige apps vragen om meer rechten dan nodig is voor het kunnen functioneren van de software. Voorbeelden hiervan zijn toegang tot contact-of andere privégegevens, rechten tot in-app aankopen, of rechten om je account of draadloze verbinding te gebruiken. Deze onnodige rechten bieden mogelijkheden tot misbruik. Dergelijke apps zijn een bekende bron van virussen en malafide software.

Neem bij twijfel contact op met de ICT servicedesk.

Het inbreken (jailbreaken) op de smartphone of tablet van je werk, om op die wijze gebruik te kunnen maken van applicaties die niet in de reguliere app-stores te verkrijgen zijn, is niet toegestaan.

1.14 Werken met Wi-Fi

In de panden van het COA is een beveiligde Wi-Fi beschikbaar. Gasten kunnen ook een tijdelijke Wi-Fi code ontvangen.

Op Rijkportaal vind je meer informatie over de Wi-FI mogelijkheden voor jouw organisatie[18].

Wees voorzichtig met Wi-FI, zowel met je eigen apparatuur als met apparatuur die je van je werk hebt ontvangen. Gratis Wi-Fi zoals vaak aanwezig is in hotels en op vliegvelden en soms in horeca gelegenheden, is veelal onbeveiligd. Ook al wordt een (tijdelijke) Wi-Fi-code verstrekt of verkocht, het berichtenverkeer via die Wi-Fi verbinding kan door onbevoegden worden afgevangen en toegankelijk worden gemaakt.

Het Nationaal Cyber Security Centrum (NCSC) geeft informatie over hoe je jouw eigen verbinding thuis kunt beveiligen en hoe je veilig met openbare Wi-Fi om kunt gaan[19].

Neem bij twijfel of vragen contact op met de ICT servicedesk.

[18] Werken met Wi-Fi;
http://portal.rp.rijksweb.nl/irj/portal/?NavigationTarget=HLPFS://cisrijksportaal/cisfacilitair/cisicteninformatievoorziening_1/ciswifi__rijksbreed_/cisveiligheid_en_trends
[19] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/wifi-onderweg-gebruik-een-vpn

1.15 Toegang en wachtwoorden zijn van jou

Bij indiensttreding ontvang je toegang (een inlogaccount) tot de digitale werkomgeving. Jouw functie en het soort informatie waarmee jij werkt, is bepalend voor welke voorzieningen nodig zijn voor jouw functie-uitoefening. Je leidinggevende stelt vast welke toegangsrechten en voorzieningen jij krijgt.
Jouw account is de sleutel tot jouw digitale werkomgeving en daarmee tot de informatie waar jij verantwoordelijk voor bent.

Jouw account is de sleutel tot jouw digitale werkomgeving en daarmee tot de informatie waar jij verantwoordelijk voor bent.

Het is verstandig om je gebruikersnaam en wachtwoorden voor de digitale werkomgeving niet voor andere al dan niet publieke sites of apps te gebruiken. Je internetbrowser biedt aan om de wachtwoorden voor je op te slaan. Dit is niet veilig!

Het is van belang dat wachtwoorden geheim blijven. Daarom is het niet handig om wachtwoorden op te schrijven.

Geef nooit je wachtwoord aan anderen; ook niet aan “beheerders”. Beheerders zullen namelijk nooit vragen om wachtwoorden.

Verander direct je wachtwoorden als je vermoedt dat iemand die heeft kunnen zien of als je vermoedt dat ze niet langer geheim zijn. Lukt dit niet, neem dan zo snel mogelijk contact op met de ICT servicedesk.
Ga zorgvuldig om met je voorzieningen en zorg ervoor dat informatie niet in handen van onbevoegden kan vallen.

Ben je even niet op je werkplek? Vergrendel de digitale werkomgeving met CTRL-ALT-DEL of schakel je werkomgeving uit, zodat er geen misbruik van gemaakt kan worden.

Je bent zelf verantwoordelijk voor de handelingen die jij verricht dan wel laat verrichten onder jouw inloggegevens en je kunt hierop worden aangesproken door je leidinggevende en door de beveiligingstoezichthouders.

Het is niet toegestaan om de inloggegevens of persoonlijke toegang tot de digitale werkomgeving van een ander te gebruiken.

Soms is het nodig, voor de continuïteit van de werkzaamheden, dat anderen bij jouw email en bestanden kunnen. Jouw inloggegevens of persoonlijke toegang delen met collega’s mag niet. In overleg met je leidinggevende kun je een collega naar eigen keuze digitaal machtigen tot het raadplegen van jouw binnengekomen berichten, onder de afspraak dat het eventuele privékarakter gerespecteerd wordt. Je collega kan op overtreding van die afspraak disciplinair aangesproken worden.

Wanneer het, vanuit het oogpunt van de continuïteit van de werkzaamheden, toch noodzakelijk is dat aan derden toegang wordt verschaft tot de digitale werkomgeving van een medewerker, dan kan de organisatie daar aanvullende procedures voor afspreken. (zie: Toegang ivm continuïteit van werkzaamheden in de toelichting op de Gedragsregeling voor de digitale werkomgeving.)

1.16 Omgang met vertrouwelijke informatie

Als medewerker heb je vaak toegang tot een veelheid aan informatie, waaronder vertrouwelijke of gevoelige informatie. Informatie kan bijvoorbeeld politiek-, commercieel- of privacygevoelig of personeelsvertrouwelijk zijn. Met al deze informatie moet op zorgvuldige wijze worden omgegaan. Hanteer de clean desk & clear screen principes: berg vertrouwelijke informatie op en vergrendel bij afwezigheid je scherm. Laat vertrouwelijke informatie niet onbeheerd achter.

Ga na of jij met gevoelige of vertrouwelijke informatie werkt en stel je op de hoogte van de geldende wetten en regels. Als je met gevoelige of vertrouwelijke informatie werkt, is het belangrijk dat jij bepaalt welke mate van vertrouwelijkheid de informatie heeft en dat je aangeeft welke mate van beveiliging daarvoor nodig is (rubriceren). Je kunt hiervoor advies vragen aan je leidinggevende of aan de CISO of privacy officer.

Informatie gebruik je alleen voor het doel waarvoor die is verstrekt en vertrouwelijke informatie deel je niet met onbevoegden.

Het verwerken van gevoelige of vertrouwelijke informatie op onveilige apparatuur (privémiddelen of voorzieningen in bijvoorbeeld openbare internetcafés) of buiten de digitale werkomgeving van COA is risicovol en is dan ook niet toegestaan. Op het moment dat privé- of openbare apparatuur geïnfecteerd is met malware is het risico dat vertrouwelijke informatie uitlekt groter. Door het – al dan niet bewust – lekken van (gevoelige of vertrouwelijke) informatie, wordt het vertrouwen in de overheid in het algemeen en jouw bewindspersoon in het bijzonder geschaad.

1.17 Verzending van vertrouwelijke informatie

Ga zorgvuldig om met het verzenden van persoonsgegevens en vertrouwelijke informatie via e-mail.

E-mail is buiten het Rijk niet beveiligd. Daarom mag je vanuit COA geen persoonsgegevens of vertrouwelijke informatie sturen naar e-mailadressen buiten het Rijk. In enkel gevallen zijn er aanvullende beveiligingsmaatregelen genomen naar specifieke e-maildomeinen[20], waardoor dit wel is toegestaan. Er is dan sprake van beveiligde e-mail (FTLS).

[20] Dit geldt bijvoorbeeld voor Arts en Zorg en het Rode Kruis. Er wordt gewerkt aan verbeterde oplossing, Zivver. Met Zivver kan straks met iedereen veilig gemaild worden indien dit noodzakelijk is.

Binnen het rijks(e-mail)domein (aan COA ketenpartners binnen JenV) mag je vertrouwelijke informatie, die op grond van de Handleiding Rubricering[21] gerubriceerd moet worden verzonden, in ieder geval tot en met het niveau Departementaal Vertrouwelijk (Dep-V) verzenden. Je moet daarbij duidelijk aangeven dat het om Dep-V informatie gaat.
Verzending binnen het rijks(e-mail)domein (aan COA ketenpartners) van gerubriceerde informatie met een hoger niveau van vertrouwelijkheid (Staatsgeheim) mag alleen met toestemming van je leidinggevende en een positief advies van de CISO.

'Rubricering van informatie is het toekennen van een standaard risicoclassificatie aan informatie door er een vertrouwelijkheidsclassificatie aan te geven. Op basis van die rubricering is het duidelijke op welke wijze je met die informatie moet omgaan en welke noodzakelijke beveiligingsmaatregelen je moet nemen. COA heeft tot nu toe alleen maar Dep-V informatie.'

Ontvang je persoonsgegevens en vertrouwelijke informatie (Dep-V)? Dan mag je die niet doorsturen, zonder akkoord van de eigenaar van het document en alleen met de aanduiding Dep-V.

'Wil iemand van buiten het Rijk aan jou persoonsgegevens of vertrouwelijke informatie sturen? Adviseer diegene dan om zelf voor veilige verzending te zorgen.'

Buiten het het rijks(e-mail)domeinis verzending van vertrouwelijke informatie alleen toegestaan indien dit voor je werkzaamheden noodzakelijk is en door je leidinggevende wordt geaccordeerd. Gerubriceerde informatie moet altijd versleuteld worden met gebruikmaking van door (de AIVD) goedgekeurde cryptomiddelen, zoals de Bestandenpostbus.

'Is het voor je werkzaamheden noodzakelijk dat dergelijke informatie naar organisaties buiten het Rijk stuurt? Dan heb je eerst akkoord nodig van je leidinggevende en van de eigenaar van de informatie. Als dit sturen van informatie vastgelegd is in de processen, is dit akkoord bevonden bij goedkeuring van dat proces en is er geen akkoord nodig bij iedere verzending. Vervolgens moet je voor digitale verzending gebruik maken van de Bestandenpostbus.'

Vraag bij twijfel advies aan de CISO.

[21] Handleiding Rubricering:
http://content.rp.rijksweb.nl/cis/content/media/rijksportaal/dgobr/organisatie___interdepartementaal_/documenten_70/ibr/Handleiding_rubricering_v28-09-2015.pdf

1.18 Vervoer informatie op betrouwbare gegevensdragers

Ga zorgvuldig om met het vervoer of het versturen van bestanden buiten het Rijk op een mobiele datadrager (cd-rom, dvd, usb-stick, etc.).

Voor het vervoeren van informatie, persoonsgegevens en informatie die op grond van de geldende Rubriceringsrichtlijn moet worden gerubriceerd (bijna alle informatie binnen het COA), mogen alleen daarvoor goedgekeurde, extra beveiligde, faciliteiten worden gebruikt, die in overleg met je leidinggevende en de CISO kunnen worden aangevraagd.

1.19 Verlies of diefstal van vertrouwelijke informatie

Als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens mogen hebben, spreken we van een datalek in het kader van de Algemene verordering gegevensbescherming[22]. Denk hierbij aan uitgelekte computerbestanden, gestolen of verloren datadragers waarop persoonsgegevens staan of wanneer bij een (digitale) inbraak dossiers met gegevens over personen (mogelijk) zijn ingezien door derden.

Ben je informatie(dragers) verloren of is er sprake van inbraak of diefstal, meld dit dan direct aan de je leidinggevende en de ICT-Servicedesk.

Doe ook aangifte bij de politie en een kopie van het proces-verbaal moet overlegd worden aan de ICT-medewerker bij uitlevering van vervangende middelen of aan de ICT-Servicedesk.

1.20 Respecteer andermans eigendommen

Respecteer auteursrechten en (intellectuele)eigendomsrechten van anderen.

Soms is een bronvermelding onvoldoende. Controleer of op de site expliciet wordt vermeld dat downloaden (wettelijk) is toegestaan, wanneer je bestanden en informatie ten behoeve van je werkzaamheden van het internet downloadt. Het downloaden van auteursrechtelijk beschermde foto's, muziek-en filmbestanden mag niet zonder toestemming van de eigenaar en is strafbaar.

[22] Datalek: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken?qa=datalek

2. Toelichting op de Gedragsregeling voor de digitale werkomgeving

Gebruik van internet en mogelijkheden voor digitaal berichtenverkeer is voor veel COA-medewerkers nodig voor het werk. Veel processen verlopen digitaal en vaak is uitwijken naar analoge processen moeilijk of niet meer mogelijk. Het COA biedt medewerkers en gasten online toegang tot bijvoorbeeld internet en mogelijkheden voor digitaal berichtenverkeer, vanuit de (mobiele) digitale werkomgevingen in kantoorlocaties, (tijdelijke) draadloze netwerktoegang of via telewerkvoorzieningen. Aan het gebruik van deze mogelijkheden zijn echter risico's verbonden. Risico's zijn bijvoorbeeld beschadiging of verlies van informatiesystemen en gegevens door onder andere virussen, inbraken door hackers of het uitlekken van gevoelige informatie. Ook kan het imago van het COA geschaad worden. Risico's ontstaan vaak onbewust door je gedrag of door ongewenst gebruik van de digitale werkomgeving. Als je informatie downloadt of bijlagen van berichten opent, kunnen onbedoeld virussen, spyware en andere kwaadaardige software meekomen of worden opgestart.

Veilig, effectief en efficiënt gebruik van de digitale werkomgeving draagt bij aan de betrouwbaarheid en weerbaarheid[23] van de informatievoorziening van het COA. Waar nodig heeft het COA daarom technische voorzieningen ingericht die er voor zorgen dat de informatie beschikbaar blijft voor het werkproces en dat de integriteit en vertrouwelijkheid van de informatie geborgd is. Niet alle risico's zijn echter technisch te ondervangen. Daarom zijn afspraken over de toegang tot en het gebruik van de digitale werkomgeving nodig.

2.1 Uitgangspunten

Eigen verantwoordelijkheid waar dat kan, regels en controle daar waar nodig, dat is het uitgangspunt. Als medewerker ben je zelf verantwoordelijk voor je gedrag op en het gebruik van die digitale voorzieningen. Daarom zul je zoveel mogelijk beschermd en toegerust moeten zijn in het omgaan met de risico's. En daarom wordt van je verwacht dat je je overeenkomstig de inhoud en de strekking van de gedragsregeling gedraagt. Onjuist omgaan met de digitale werkomgeving kost tijd en capaciteit van mensen en apparatuur en kan tot onnodig hoge kosten leiden.

[23] Weerbaarheid is het vermogen van de digitale werkomgeving om weerstand te bieden tegen voorstelbare dreigingen.

Daarbij werk je met overheidsinformatie. De informatie die je voor je werk ontvangt, opmaakt of verzendt komt in aanmerking om direct of op termijn openbaar gemaakt te kunnen worden[24] en wordt duurzaam toegankelijk gehouden. Gebruik maken van de geboden internetfaciliteiten betekent dat je instemt met logging (registreren) en de mogelijkheid tot monitoring (bekijken) van het internetgebruik door ICT conform de daarvoor geldende regels en procedures.

2.2 Privacy en privégebruik

Gepast privégebruik mag. Misbruik, dat wil zeggen overmatig, uitbundig, storend of schadelijk privégebruik, is niet toegestaan. Op basis van de begrippen goed werknemerschap en goed werkgeverschap moeten beide partijen zich houden aan zowel verantwoord gebruik van e-mail en internet als aan een zorgvuldig controlebeleid. De Algemene verordening gegevensverwerking (AVG)[25] geeft het kader aan hoe rondom het gebruik van het internet en digitaal berichtenverkeer met persoonsgegevens moet worden omgegaan, zodat jouw privacy geborgd is. In deze Gedragsregeling zijn de regels van de Autoriteit Persoonsgegevens[26] als uitgangspunt genomen. Jouw organisatie is verantwoordelijk voor het opstellen van aanvullende regelingen, zoals een organisatie privacy verklaring, waarin is vastgelegd hoe omgegaan wordt met jouw privacy en je gebruiks-en verkeersgegevens.

2.3 Integriteit en online gedrag

Het internet is een open infrastructuur die voor iedereen toegankelijk is. Je moet je ervan bewust zijn dat je voor anderen herkenbaar kunt zijn als een medewerker van het COA, doordat bij iedere activiteit het IP-adres te achterhalen is (de identiteit van het device). In de Uitgangspunten online communicatie rijksambtenaren[27] wordt toegelicht waar de grenzen liggen van activiteiten op het web en de scheiding tussen werk en privé. Uitgangspunt is, dat zaken 'online' op dezelfde manier worden behandeld als 'offline'. Wees altijd zorgvuldig, betrouwbaar, integer en respectvol. Alle informatie die je genereert, ontvangt of verzamelt in het kader van de uitvoering van je taak, is en blijft eigendom van de overheid.
Je hebt als COA-medewerker een Geheimhoudingsplicht: dus vertrouwelijke informatie blijft vertrouwelijk. Dit betekent niet alleen dat je geen informatie 'lekt', maar ook dat je zorgvuldig omgaat met informatie en informatiedragers. Het betekent, dat jij je bewust bent van en rekening houdt met de aard en mogelijke impact van de informatie waarover je beschikt en je bewust bent van de risico's.

[24] In het kader van de Wet openbaarheid van bestuur, de Archiefwet, de Baseline Informatiebeveiliging Rijksdienst en volgens de richtlijnen in de E-mailgedragslijn Baseline (versie 1.0, 080701)
[25] Algemene Verordening Gegevensbescherming: https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
[26] https://www.autoriteitpersoonsgegevens.nl/nl/onderwerpen/werk-uitkering/controle-van-personeel
[27] Uitgangspunten online communicatie rijksambtenaren: https://www.rijksoverheid.nl/documenten/rapporten/2010/06/30/uitgangspunten-online-communicatie-rijksambtenaren

Bovenstaande is ook opgenomen in de Gedragscode Integriteit COA[28] en de Gedragsrichtlijnen Social Media, waarin het algemene kader is beschreven voor integer handelen binnen de rijksoverheid. Zo zijn onder andere gedragsregels opgenomen over informatie en communicatie, waar onder online communicatie en sociale media en over het gebruik van middelen en voorzieningen. Deze Gedragsrichtlijn voor de digitale werkomgeving is een nadere uitwerking van integere omgang met de mogelijkheden van de digitale werkomgeving en online gedrag.

2.4 Inbreuk op de Gedragsregeling

Als je de regels met betrekking tot integriteit overtreedt, wordt dit beschouwd als plichtsverzuim. Dat geldt ook voor inbreuk op deze Gedragsregeling. Dit kan verschillende sancties en maatregelen tot gevolg hebben, afhankelijk van de aard en ernst van het vastgestelde plichtsverzuim. Bij ernstige inbreuk op deze Gedragsregeling zal het bestuur op de hoogte worden gesteld van het incident.
Voordat tot het opleggen van een sanctie wordt overgegaan, zal altijd eerst gedegen onderzoek moeten plaatsvinden. De feiten moeten op deugdelijke wijze worden vastgesteld en er moet rekening worden gehouden met relevante omstandigheden. Daarbij moet sprake zijn van hoor en wederhoor, zorgvuldige verslaglegging en – voor zover van toepassing -een evenredige inzet van onderzoeksmiddelen.
In geval van niet-ambtenaren kunnen maatregelen worden genomen conform de contractuele afspraken op dit gebied. Aangifte bij de politie behoort eveneens tot de mogelijkheden.

2.5 Uitzonderingen

Indien er zich situaties voordoen waarin deze Gedragsregeling niet voorziet, zal conform het arbeidsrechtelijk kader en de AVG, en indien nodig in overleg met de ondernemingsraad, worden gehandeld.

2.6 Werking

Deze Gedragsregeling bepaalt het minimumkader dat COA-breed van toepassing is. Met de inwerkingtreding van deze Gedragsregeling vervallen de bestaande regelingen van de organisaties binnen het COA en treedt deze COAbrede regeling daarvoor in de plaats.
Onderdelen binnen het COA mogen een aanvullende gedragsregeling opstellen waarin zij deze Gedragsregeling waar nodig nader specificeren. Onderdelen mogen daarbij wel strikter, maar niet ruimer zijn in hun normering dan de Gedragsregeling als COA-breed kader aangeeft.
Deze Gedragsregeling is van toepassing op iedereen die gebruik maakt van de digitale faciliteiten van het COA en is ook van toepassing op het werkgerelateerde online verkeer via privé-middelen. Deze Gedragsregeling geldt voor alle COA-medewerkers en externen en is ook van toepassing op thuis- of telewerken.

[28] Gedragscode Integriteit: https://plein-intranet.coa.local/HRO/geni/Paginas/Integer-werken.aspx

Het COA vraagt ook dat externen zich in lijn met deze Gedragsregeling gedragen en handelen. Als je ingehuurd bent, geen ambtelijke aanstelling hebt en wel de beschikking krijgt over digitale faciliteiten, ben je contractueel aan deze Gedragsregeling gebonden. In het individuele contract dat met jou wordt gesloten, is een bepaling opgenomen op grond waarvan je gebruik mag maken van de digitale faciliteiten en je verplicht wordt om de Gedragsregeling na te leven.

Gasten worden ook op de hoogte gesteld van de voor hen geldende regels, bijvoorbeeld bij het moment van beschikbaar stellen van wifi-codes voor tijdelijke toegang of bij het inloggen op het wifi-netwerk.

3. Aanvullende informatie over beheer en controle van de voorzieningen

De digitale werkomgeving wordt beheerd door de systeem- en netwerkbeheerders van de ICT-beheerorganisatie van het COA. Alleen onder strikte voorwaarden hebben zij voor hun werkzaamheden toegang tot de systemen en de informatie die daar in zit.

Het COA treft voorzieningen om de positie en integriteit van de systeem- en netwerkbeheerders van de ICT-beheerorganisaties te beschermen en controleert daarop. In een Protocol voor beheerders beschrijft de ICT-beheerorganisatie aanvullende gedragsregels over hoe beheerders om moeten gaan met de bijzondere rechten die zij hebben voor het beheer van de digitale werkomgeving.

Waar nodig heeft het COA technische voorzieningen ingericht die er voor zorgen dat de informatie beschikbaar blijft voor het werkproces en duurzaam toegankelijk kan worden gehouden. De back-up procedure biedt blijvend betrouwbare back-ups.

3.1 Logging, monitoring en controle

Het COA zou mogelijk een doelwit van geavanceerde digitale aanvallen voor spionage, sabotage of zelfs terrorisme kunnen zijn. Daarom heeft het COA technische voorzieningen ingericht die de betrouwbaarheid en weerbaarheid van de informatievoorziening van het COA waarborgen. Voor het opsporen en buiten werking stellen van virussen, spyware en andersoortige kwaadaardige programma's wordt onder andere gebruik gemaakt van virusscanners en meer geavanceerde sensoren.

Om technische fouten en onregelmatigheden vroegtijdig te ontdekken en tijdig onderhoudsmaatregelen te kunnen treffen (preventieve maatregel), wordt zowel het gebruik als de werking van de digitale werkomgeving en de internetfaciliteiten geautomatiseerd vastgelegd (gelogd). Deze automatische logging van de werking van de ICT-middelen (apparatuur en programmatuur) door de ICT-beheerorganisatie vindt permanent plaats. Het logbestand wordt gebruikt om de werking van de voorzieningen te onderhouden. Deze logging is beperkt.

Het bestuur vindt een goede balans belangrijk tussen enerzijds controle op verantwoord berichtenverkeer- en internetgebruik en anderzijds bescherming van jouw privacy op de digitale werkomgeving.

Het logbestand zal alleen worden gebruikt voor nader onderzoek naar het gebruik, mits daarvoor formeel opdracht gegeven is door het bestuur (correctieve maatregel).

De monitoring van het berichtenverkeer en internetgebruik vindt op geautomatiseerde wijze plaats en is niet-persoonsgericht. Monitoring is gericht op beveiliging en bedoeld voor technisch onderhoud van het systeem en het netwerk. Deze niet-persoonsgerichte monitoring gebeurt ook ter voorkoming en detectie van overtreding

van de gedragsregels. Hiermee kunnen afwijkingen in het internetverkeer waargenomen worden die op een veiligheidsrisico kunnen duiden.

De controle op het berichtenverkeer en internetgebruik is niet-persoonsgericht, maar wel een verwerking van persoonsgegevens in de zin van de Algemene verordening gegevensbescherming (AVG). Deze controle wordt daarom door de ICT-beheerorganisatie op zodanige wijze uitgevoerd dat de fundamentele rechten en vrijheden van betrokken werknemers, in het bijzonder het recht op bescherming van de persoonlijke levenssfeer in acht worden genomen. De controle wordt beperkt tot het vooraf geformuleerde doel en door middel van op die doeleinden toegesneden controlemechanismen.

In het COA privacybeleid en -verklaring is vastgelegd hoe COA omgaat met jouw gebruiks- en verkeersgegevens.

3.2 Persoonsgerichte inhoudelijke controle

Inhoudelijke controle van het internet- en berichtenverkeer kan alleen plaatsvinden indien sprake is van een redelijk vermoeden van een integriteitschending of ander plichtsverzuim.

Na een melding van dit vermoeden aan het bestuur kan deze bij zwaarwegende redenen besluiten tot een gericht digitaal integriteitonderzoek achteraf van de door die medewerker verrichte verwerkingen met de berichten en internetvoorzieningen, ter beoordeling in hoeverre de rechtspositieregels in de Ambtenarenwet, de Gedragscode Integriteit COA, de Gedragsrichtlijnen Social media of deze Gedragsregeling is of wordt overtreden.

Een gericht digitaal integriteitonderzoek is een door een directeur en bestuur goedgekeurd diepgaand digitaal onderzoek, met een vastgestelde scope en onderzoeksdoel, naar het gebruik van door de werkgever verstrekte ICT-faciliteiten door een specifieke medewerker of medewerkers, aan de hand van digitale informatie m.b.t. dat gebruik[29].

Wat wordt onderzocht en hoever het onderzoek reikt, is altijd proportioneel. Persoonsgegevens gerelateerd aan berichtenverkeer-en internetgebruik worden niet langer gebruikt dan noodzakelijk. Tot jou herleidbare gegevens die gerelateerd zijn aan jouw gebruik van het berichtenverkeer en de internetvoorzieningen, kunnen ten behoeve van controle langer worden gebruikt, indien wordt besloten tot de controle en voor zover dat noodzakelijk is voor die controle.

[29] Een gericht digitaal integriteitonderzoek is niet hetzelfde als digitaal forensisch onderzoek waarbij digitale sporen worden onderzocht ten behoeve van strafrechtelijk onderzoek waarbij daders of oorzaken van (mogelijke) misdrijven worden opgespoord op basis van wetenschappelijk bewijs. Gericht digitaal integriteitonderzoek gaat veel minder ver, maar kan in sommige gevallen wel uitmonden in digitaal forensisch onderzoek. In dat geval worden gebruiksgegevens overgedragen aan bevoegd gezag (OM).

3.3 Toegang i.v.m. continuïteit van werkzaamheden

Als je langdurig niet aanspreekbaar bent, bijvoorbeeld door ziekte, langdurige vakantie of detentie of andere vormen van langdurige afwezigheid, dan kan het noodzakelijk zijn dat aan derden toegang wordt verschaft tot jouw inlog-account en digitale werkomgeving, vanuit het oogpunt van de continuïteit van de werkzaamheden. Voor die situatie geldt een noodprocedure[30].

Als de toegang noodzakelijk is, kan je direct leidinggevende onderbouwd bij de ICT-Servicedesk toegang vragen tot je Digitale werkomgeving. Je direct leidinggevende zal eerst jouw toestemming vragen. In overleg met de privacy officer zal je leidinggevende een afweging maken tussen het belang van de dienst en het belang van jouw privacy. Je direct leidinggevende stelt jou en de CISO daarna van het besluit in kennis. In geval van jouw overlijden kan je leidinggevende onderbouwd samen met de privacy officer vanuit het vier-ogenprincipe toegang tot jouw Digitale werkomgeving verkrijgen. In al deze situaties wordt in principe alleen gekeken naar werk-gerelateerde informatie.

[30] Procedure 'Verlenen tijdelijk toegang tot e-mailboxen van medewerkers' van de ICT-Servicedesk.

4. Verplichte Basiscursus

Integer handelen is essentieel verbonden aan het functioneren als ambtenaar. Een goede omgang met informatie is hierbij van groot belang. Om medewerkers[31] hierbij te ondersteunen biedt de werkgever de basiscursus risicobewust handelen "Hoe alert ben jij" aan. Medewerkers zijn verplicht deze cursus jaarlijks te volgen.
Reden van deze basiscursus is dat ieder wordt geacht kennis te nemen van de risico's die bestaan bij het omgaan met (digitale) gegevens en voorzieningen. De cursus is ervoor om als medewerker meer van de risico's bewust te zijn, daar meer alert op te zijn en te leren hoe daarmee om te gaan.

Aangezien dit binnen het ministerie van Justitie en Veiligheid, en ook in de maatschappij als geheel steeds belangrijker wordt, is deze cursus voor iedere medewerker binnen het ministerie van Justitie en Veiligheid verplicht gesteld, inclusief uitvoeringsorganisaties en ZBO's die onder het ministerie vallen.

De cursus is in beginsel alleen online te volgen en duurt één uur. Medewerkers dienen de cursus ieder jaar te volgen, om op de hoogte te blijven van de meest actuele risico's en de wijze waarop hiermee om te gaan.

De medewerker overlegt met diens leidinggevende op welk moment de cursus gevolgd wordt. Dat is in beginsel onder werktijd. Mocht dit niet mogelijk zijn en moet de cursus buiten werktijd worden gevolgd, dan maakt de medewerker met de leidinggevende afspraken over de compensatie hiervan. In het geval van een toename van risico's kan de cursus door de werkgever worden uitgebreid en meer tijd in beslag nemen.

De medewerker is zelf verantwoordelijk voor het (tijdig) volgen van de cursus. Tijdens het voor- of najaargesprek zal het al dan niet gevolgd hebben van de cursus aan bod komen. Via het COA-Leerplein is inzichtelijk welke opleidingen een medewerker gevolgd heeft via het Leerplein.

Gelet op het belang dat het COA hecht aan het volgen van de cursus, kan het niet volgen daarvan – zonder redelijke grond – arbeidsrechtelijke consequenties voor u hebben en zo nodig tot sancties leiden

[31] Onder medewerkers worden zowel interne als ingehuurde externe medewerkers verstaan.