Protocol Automatiseringsmiddelen 2024

3 juni 2024
Versie 1.1
Definitief

Inhoud

1 Inleiding

1.1 Doel

Het protocol brengt de voorschriften en instructies samen die voor medewerkers van de gemeente Utrecht gelden op het gebied van het gebruik van automatiseringsmiddelen en gegevens en is daarmee onderdeel van het Handboek Utrechts Personeel (HUP). De gemeente Utrecht doet dit vanuit haar rol als werkgever.

1.2 Uitgangspunten

1.2.1 De gemeente heeft beleid op het gebied van gegevensbescherming. Dit beleid gaat onder meer over het beschermen van gegevens van inwoners, ondernemers en medewerkers van de gemeente en wat hier de gemeente hiervoor doet. Onderdeel van het beleid is dit protocol.

1.2.2 Dagelijks worden in ons werk gegevens gemaakt en gebruikt. In dit protocol staat hoe om te gaan met automatiseringsmiddelen en gegevens. Het bevat instructies aan medewerkers hoe ze met automatiseringsmiddelen en gegevens om moeten gaan en waarom. Als een medewerker zich niet aan de instructies houdt kan dit consequenties hebben. In het HUP zijn hiervoor regels opgenomen in het hoofdstuk integriteit.

1.2.3 Als gemeente beschikken wij over veel gegevens van inwoners en ondernemers die beschermd moeten worden. Ook hebben wij als gemeente vergaande bevoegdheden en vaak een monopoliepositie. Inwoners kunnen niet ons ons heen. Onze inwoners en ondernemers mogen dus een integere gemeente verwachten die zorgvuldig en integer omgaat met hun (persoons)gegevens.

1.2.4 Het protocol geldt voor alle vaste en tijdelijke medewerkers, zowel intern als extern, van de gemeente Utrecht. Hieronder verstaan wij ook stagiaires, uitzendkrachten, payrollers, consultants, schoonmaak- en cateringpersoneel, freelancers, interimmanagers en vrijwilligers.

1.2.5 Naast dit protocol kunnen er specifieke instructies of regels zijn die voor jouw afdeling of werkzaamheden gelden. Je handelt in overeenstemming met deze instructies en regels. Je leidinggevende kan je hierbij helpen en kan je vragen beantwoorden.

1.2.6 Dit protocol wordt vastgesteld door de Directieraad. Na vaststelling hiervan, vervallen eerdere versies van het protocol. Het protocol wordt één keer per twee jaar volledig gereviewd en op onderdelen eerder als hier aanleiding toe is.

1.3 Definities en afkortingen

1.3.1	*account*	Een persoonlijke set aan rechten om gebruik te maken van bepaalde automatiseringsmiddelen en/of gegevens. Bevat daarnaast een profiel van de gebruiker met haar of zijn persoonlijke gegevens. Gebruik van een account kan worden beveiligd met inloggegevens zoals een gebruikersnaam en wachtwoord. Aan het gebruik van een account zijn regels verbonden. Het wachtwoord moet geheim blijven en toegekende rechten mogen alleen gebruikt worden voor de uitvoering van de werkzaamheden.
1.3.2	*apparatuur*	Computers, laptops, telefoons, tablets, gegevensdragers, randapparatuur en onderdelen.
1.3.3	*automatiserings-middelen*	Alle apparatuur en software.
1.3.4	*AVG*	Algemene verordening gegevensbescherming, ook bekend als General Data Protection Regulation (GDPR). Europese privacywetgeving.
1.3.5	*datalek*	Een datalek is een gegevensbeschermingsincident dat mogelijk betrekking heeft op persoonsgegeven(s) met als mogelijk gevolg: vernietiging, verlies, wijziging, ongeoorloofde verstrekking van de gegevens of ongeoorloofde toegang daartoe. Bijvoorbeeld: Verlies van persoonsgegevens door het kwijtraken van een USB-stick, zonder back-up van de gegevens. Twijfel over

		betrouwbaarheid van de gegevens, zoals onzekerheid over versie, echtheid, compleetheid, samenhang of originaliteit. Een gebrek in de afscherming van persoonsgegevens, waardoor de vertrouwelijkheid mogelijk is geschonden.
1.3.6	*de gemeente*	De gemeente Utrecht in haar rol als werkgever.
1.3.7	*Digitale Werkplek*	De Digitale Werkplek van de gemeente bestaat uit zakelijke apparatuur (zoals een zakelijke laptop of kantoorwerkplek), het netwerk waarop je inlogt en de cloudomgevingen van de gemeente (zoals Teams).
1.3.8	*DISO*	Decentrale Information Security Officer. De DISO is voor iedereen in haar of zijn organisatieonderdeel de adviseur over privacy en informatiebeveiliging en is hierin onafhankelijk. Op intranet vind je een overzicht van de DISO's per organisatieonderdeel.
1.3.9	*DPIA*	Data Protection Impact Assessment: analyse van de privacyaspecten van een proces.
1.3.10	*Duurzaam toegankelijke informatie*	Informatie is vindbaar, beschikbaar, leesbaar, interpreteerbaar, betrouwbaar en toekomstbestendig. Meer over duurzaam toegankelijke informatie lees je hier.
1.3.11	*Gedragscode*	De gedragscode integriteit zoals genoemd in het Handboek Utrechts Personeel.
1.3.12	*gegevens*	Ook wel data en informatie. Dit kunnen zowel persoonsgegevens zijn, of bijvoorbeeld gegevens die worden gebruikt in de bedrijfsvoering zoals documenten of dossiers.
1.3.13	*gegevensbeschermings-incident*	Een gegevensbeschermingsincident is een gebeurtenis die tot gevolg kan hebben dat de informatie van de gemeente onbedoeld of ongeautoriseerd: ontoegankelijk wordt gemaakt (niet langer beschikbaar is, een aantasting van de beschikbaarheid), wordt gewijzigd (niet langer integer is, een aantasting van de integriteit), of wordt ingezien (niet langer vertrouwelijk is, een aantasting van de vertrouwelijkheid). Dit kan om informatie gaan in alle vormen, waaronder in systemen, op gegevensdragers, op papier of in de hoofden van mensen.
1.3.14	*gegevensdrager*	Alle apparatuur waar gegevens op kunnen staan.
1.3.15	*Handboek Utrechts Personeel (HUP)*	De regels die voor alle gemeenteambtenaren in Nederland gelden staan in de Cao Gemeenten. De Utrechtse afspraken die alleen voor werknemers van de gemeente Utrecht gelden staan in het Handboek Utrechts Personeel (HUP)
1.3.16	*informatie*	(Persoons)gegevens in welke vorm dan ook die onder het beheer van de gemeente vallen.
1.3.17	*informatiebeheer*	Informatiebeheer richt zich op het duurzaam toegankelijk maken van informatie, dat wil zeggen: het vindbaar, beschikbaar, leesbaar, interpretabel, betrouwbaar, en toekomstbestendig maken en houden van informatie zodat deze informatie optimaal (her)bruikbaar is, voor hen die daar recht op hebben. Processen daarbinnen zijn: registreren, vernietigen, migreren, ter beschikking stellen en bewaren.
1.3.18	*informatiebeveiliging*	Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.
1.3.19	*informatieproces*	Een proces waarin informatie wordt verwerkt, opgeslagen, gearchiveerd of verwijderd.
1.3.20	*inwoners*	De inwoners van de gemeente Utrecht.

1.3.21	*IPM*	Informatie en Proces Manager. De IPM is voor iedereen in haar of zijn organisatieonderdeel de adviseur over automatiseringsmiddelen en informatieprocessen.
1.3.22	*IRM*	Integraal Resultaatverantwoordelijk Manager. De IRM is integraal verantwoordelijk voor zijn eigen organisatieonderdeel.
1.3.23	*medewerker*	In het kader van dit protocol wordt onder medewerker verstaan alle vaste en tijdelijke medewerkers, zowel intern als extern, van de gemeente Utrecht. Ook stagiaires, uitzendkrachten, payrollers, consultants, bewakings- schoonmaak- en cateringpersoneel, freelancers, interimmanagers en vrijwilligers vallen onder dit begrip.
1.3.24	*mobiele gegevensdrager*	Gegevensdragers die makkelijk meegenomen kunnen worden, zoals laptops, losse harde schijven en USB-sticks.
1.3.25	*persoonsgegevens*	Elk gegeven wat in verband kan worden gebracht met een natuurlijk persoon (bijvoorbeeld: naam of persoonsnummer) of waarmee een persoon herleid kan worden (bijvoorbeeld: kenteken of postcode).
1.3.26	*RM*	Recordmanager. De RM is voor iedereen in haar of zijn organisatieonderdeel de beheerder of adviseur op het gebied van informatiebeheer. Dit bestaat onder andere uit het gebruik van informatie in bedrijfsprocessen (verwerken, opslaan, archiveren, verwijderen), relevante interne regelgeving en wetgeving. Klik hier voor een overzicht met de recordmanagers.
1.3.27	*sleutelfunctie*	Een sleutelfunctie binnen een organisatie is een functie waarvan de mailbox, gezien zijn positie in de organisatie, geldt als een belangrijk informatieknooppunt
1.3.28	*software*	Ook wel programmatuur. Computerprogramma’s zoals een besturingssysteem van een pc of laptop (bijvoorbeeld Windows of macOS), telefoon of tablet (bijvoorbeeld Android of iOS) en applicaties (apps) die hierop worden gebruikt.

2 Dagelijks gebruik

In dit hoofdstuk worden de voorschriften en instructies behandeld die terugkomen in het dagelijks gebruik van automatiseringsmiddelen.

2.1 Veilig gedrag

2.1.1 Er is een gedragscode van toepassing voor iedereen die werkt voor de gemeente. De gedragscode schrijft voor hoe integer te handelen en is uiteraard ook van toepassing bij het gebruiken van automatiseringsmiddelen en gegevens. Op Sharepoint kan je de gedragscode terugvinden.

2.1.2 Wees bewust wanneer je werkt met vertrouwelijke gegevens en handel hiernaar, wat dit precies betekent volgt hierna.

2.1.3 Volg trainingen en instructies over gegevensbescherming en informatiebeheer zoals de E-learning Gegevensbescherming en De gouden regels voor informatiebeheer.

2.1.4 Heb je vragen over veilig gedrag? Je kan contact opnemen met de DISO van je organisatieonderdeel, waarvan op Sharepoint een overzicht is gepubliceerd. De DISO kent de wetten, regels en het gemeentelijke beleid voor privacy en informatiebeveiliging.
Voor vragen over automatiseringsmiddelen en informatieprocessen kan je terecht bij de IPM-er van je organisatieonderdeel. Ook hiervan is op Sharepoint een overzicht gepubliceerd.

2.1.5 Laat niemand met je scherm meekijken of meeluisteren met vertrouwelijke gesprekken. Zeker op openbare locaties of in het openbaar vervoer moet bewust (en) voorzichtig worden gewerkt.

2.1.6 Vergrendel je Digitale Werkplek altijd als je je werkplek verlaat (toets Windows teken + L) en zorg dat je applicaties vooraf sluit bij schermdelen om te voorkomen dat je gegevens onbedoeld deelt. Dit noemen wel ook wel “clear screen” beleid. Hiermee verzeker je dat niemand anders dan jezelf, per ongeluk of met opzet, ongeautoriseerde toegang krijgt tot gegevens van jezelf of van de gemeente.

2.1.7 Laat geen gevoelige, zakelijke gegevens onbeschermd achter op je werkplek. Berg deze gegevens op een passende manier op of neem deze mee. Dit noemen wel ook wel “clear desk” beleid. Hiermee voorkomen we dat onbevoegden fysieke toegang tot en inzage in deze gegevens kunnen krijgen.

2.1.8 Maak geen opnames van gesprekken tenzij dit een afgestemd onderdeel is van de procedure of proces zoals bijvoorbeeld bij raadsvergaderingen. Opnames kunnen (onbedoeld) worden opgeslagen of verspreid en daarmee een potentieel privacy- of beveiligingsrisico vormen.

2.1.9 Reageer nooit op berichten met inhoud die je niet kent, vertrouwt of verwacht. Ga dus niet in op (losgeld)vragen of dreigementen. Voorbeelden van deze berichten zijn:

- Een ongevraagde e-mail van het Serviceplein om mee te kijken op je scherm.
- Een uitnodiging om te klikken op een onbekende link.
- Toegestuurde bijlages die je niet bekend voorkomen.

E-mailadressen kunnen ‘gespoofd’ worden, wat inhoudt dat het lijkt of de mail komt van een normaal e-mailadres, maar in werkelijkheid van een crimineel afkomstig is. Open deze niet en verwijder (e-mail) of sluit (websites) deze als je dit vooraf niet zag.

Meer informatie over het herkennen van spam en phishingberichten vind je hier. Ontvang je een dergelijk bericht, maak een melding bij het serviceportaal en blokkeer het nummer/e-mailadres van de afzender.

2.2 Accounts

2.2.1 Jouw accounts zijn alleen bedoeld voor persoonlijk gebruik. Jij bent verantwoordelijk voor alle acties die vanuit jouw accounts worden uitgevoerd. Houd daarom je inloggegevens geheim en leen deze niet uit.

2.2.2 Laat niemand (ook geen collega) werken onder jouw account en werk zelf ook niet met het account van een ander. Als je wilt dat een collega verantwoordelijkheden of werkzaamheden van je

overneemt kun je ze in veel gevallen machtigen, zodat ze hiervoor hun eigen account moeten gebruiken. Kom je daar niet uit, bespreek dit dan met je IPM.

2.2.3 Voor het gebruik van sommige soorten accounts gelden specifieke regels. Hiervoor zal je op de hoogte worden gesteld vooraf of tijdens het gebruik hiervan. Volg deze regels op. In bepaalde gevallen wordt gevraagd hiervoor een afzonderlijke verklaring te ondertekenen.

2.2.4 Gebruik voor zakelijke applicaties uitsluitend je zakelijke e-mailadres. Het gebruiken van je zakelijke e-mailadres voor accounts die je voor persoonlijke doeleinden gebruikt is niet toegestaan.

2.3 Wachtwoorden

2.3.1 Je moet zelf je wachtwoord instellen voor je accounts. Hiervoor gelden de volgende regels:

- De lengte is minimaal 12 tekens.
- Het wachtwoord bestaat uit tekens uit ten minste drie van de vier volgende karaktersets: kleine letters, hoofdletters, cijfers en/of speciale tekens ((({}[],.<>;:'"?/|\`~!@#$%^&*()_-+=).
- Het wachtwoord bevat niet de voor- of achternaam van de natuurlijke persoon die de gebruiker is.

2.3.2 Maak op basis van de onder 2.3.1 genoemde regels een wachtwoord dat moeilijk te raden is door anderen. Dit doe je, door geen gegevens te gebruiken die direct met jou in verband kunnen worden gebracht, zoals je verjaardag, namen van gezinsleden, de naam van je hond of de sport die je speelt.

2.3.3 Gebruik voor verschillende accounts verschillende wachtwoorden: geen hergebruik dus van hetzelfde wachtwoord voor meerdere accounts. Het is zeker belangrijk om verschillende wachtwoorden voor werk en privé (zoals je Facebook of LinkedIn) te gebruiken.

2.3.4 Maak gebruik van een wachtwoordkluis om ervoor te zorgen dat je wachtwoorden niet vergeet. Dit is software waarin je op een veilige en overzichtelijke wijze je accounts en wachtwoorden kan opslaan. De gemeente biedt dit aan voor gebruik in de Digitale Werkplek, je kan dit via het serviceplein aanvragen. Als je je wachtwoorden op een andere manier veilig houdt, berg het goed op en zorg er dan voor dat ze voor anderen écht niet te vinden en te lezen zijn.

2.3.5 Wanneer je weet of vermoedt dat een wachtwoord bij anderen bekend is, wijzig dit wachtwoord dan direct.

2.3.6 Leen je wachtwoord of token niet uit aan andere personen. Ook de IT-specialisten van de gemeente, zoals die van het serviceplein, zullen hierom nooit vragen. Wordt hierom wel door iemand gevraagd? Negeer dan dit verzoek en maak in plaats daarvan melding van een beveiligingsincident (zie 4.1).

2.4 Werken op afstand

2.4.1 Voor het werken van een andere locatie dan op kantoor/werklocatie is als uitgangspunt bepaald dat de leidinggevende en medewerker samen afspraken maken over hoe, waar en wanneer het werk wordt uitgevoerd. Het werk is daarbij bepalend. Het is de taak van de leidinggevende om te sturen op de kwaliteit, aard en inhoud van het werk. Als het werk dit vereist kan van de medewerker verwacht worden dat de medewerker op een werklocatie aanwezig is. Het uitgangspunt is van toepassing werken op alle niet-werklocaties (binnen- of buitenland, thuis of elders).

2.4.2 Werk thuis of op een locatie buiten de gemeentelijke gebouwen met de door de gemeente geleverde apparaten, indien beschikbaar.

2.4.3 Gebruik up-to-date apps en een goed beveiligde computer en thuisnetwerk als je een eigen apparaat gebruikt.

2.4.4 Verstuur geen gegevens van de gemeente, zoals dossiers of documenten, naar je (thuis)privé e-mailadres. Deze gegevens mogen niet worden opgeslagen buiten de Digitale Werkplek.

2.5 Gebruik van automatiseringsmiddelen in het buitenland

2.5.1 Door wet- en regelgeving is werken vanuit het buitenland slechts in een beperkt aantal landen toegestaan. Dit geldt ook voor incidenteel werken (bijvoorbeeld lezen van mail) gedurende vakantie/vrije tijd.

2.5.2 Werken vanuit de volgende landen is toegestaan:

- Alle landen die behoren tot de Europese Economische Ruimte (EER). Bij de EER horen alle EU-landen plus Liechtenstein, Noorwegen en IJsland. Een actueel overzicht is te allen tijde hier te vinden.
- Alle landen waarover de Europese Commissie een zogenaamd adequaatheidsbesluit heeft genomen. Het betreft o.a. de landen Argentinië, Israël, Japan, Nieuw-Zeeland, Verenigd Koninkrijk, Zwitserland en Zuid-Korea. Een actueel overzicht is te allen tijde hier te vinden.

2.5.3 De leidinggevende kan bij uitzondering toestemming geven voor het werken vanuit een ander land dan hiervoor genoemd, op voorwaarde dat de leidinggevende vooraf advies inwint bij de DISO van het organisatieonderdeel, alsook de CISO én de aard van de werkzaamheden aantoonbaar in verhouding is met de veiligheid van de te verwerken persoonsgegevens en/of bedrijfsgevoelige informatie.

2.6 Werken vanuit het buitenland op verzoek van de medewerker

2.6.1 Een medewerker kan een verzoek doen om vanuit het buitenland te werken. Er is hiervoor een aparte richtlijn van toepassing. Meer informatie daarover is hier te vinden op Sharepoint.

2.7 Internet

2.7.1 Als je werkt binnen een van de gemeentelijke gebouwen mag je incidenteel en kortstondig gebruik maken van internet voor persoonlijke doeleinden, mits het niet storend is voor de dagelijkse werkzaamheden en het netwerk te zwaar belast zoals bijvoorbeeld veelvuldig video's streamen.

2.7.2 Het is niet toegestaan om, vanuit de Digitale Werkplek of met andere zakelijke apparatuur, websites te bezoeken die:

- Pornografisch, racistisch, discriminerend, beledigend of aanstootgevend materiaal bevatten.
- In strijd zijn met de wet of ethisch handelen.
- Gokken of handel (bijvoorbeeld in aandelen, opties, cryptovaluta) faciliteren.

2.7.3 De Gedragscode beschrijft wat we van elkaar mogen verwachten als het gaat om integer gedrag.

2.8 Vergaderen en chatten

2.8.1 Video-vergaderen, chatten, groepsbellen en samenwerken doen we behulp van de producten van Office 365 (Teams, Outlook, Sharepoint en OneDrive). Handleidingen vind je hier.

2.8.2 Het is niet toegestaan om met de vergadertools opnames van videogesprekken en/of bijeenkomsten te maken tenzij dit in de procedure is vastgelegd en afgestemd zoals bijvoorbeeld bij raadsvergaderingen.

2.8.3 Vergadertools zijn vaak niet aangewezen als een archiefomgeving omdat er specifieke eisen voor de inrichting gelden. Bewaar informatie/documenten bij het (zaak)dossier in een omgeving die wel voldoet aan de eisen of creëer een (zaak)dossier op de correcte wijze. Als je niet weet hoe of waar dat moet: raadpleeg dan jouw IPM-team.

2.9 Gebruik van e-mail en berichtenapps

2.9.1 Rondom het gebruik van je zakelijke e-mailbox (bijvoorbeeld ...@utrecht.nl) en afdelingsmailbox gelden regels waaraan je je moet houden. De Regels Mailbox kan je via Sharepoint terugvinden.

2.9.2 De helft van de datalekken heeft foute e-mailadressering als oorzaak. Let dus op de juiste e-mailadressering, zeker bij het versturen van gevoelige gegevens.

2.9.3 Voor het versturen van e-mail met gevoelige inhoud, zoals persoonsgegevens of bijlagen, moet je, zowel intern als extern, gebruik maken van de oplossing voor veilig mailen. Deze functionaliteit is geïntegreerd in Outlook en zorgt voor extra beveiliging. Op Sharepoint kan je een handleiding terugvinden voor veilig mailen.

2.9.4 Gebruik je zakelijke@utrecht.nl e-mailadres niet voor persoonlijke doeleinden. Maak hiervoor gebruik van je privé e-mailadres.

2.9.5 Maak geen onnodig gebruik van de “Allen beantwoorden” functionaliteit bij e-mails aan grote groepen mensen. Gevoelige gegevens kunnen onbedoeld bij grote groepen mensen terecht komen.

2.9.6 Bij het verzenden van e-mails of chats gebruik je zo veel mogelijk linkjes/verwijzingen naar eventuele bijlagen, en verzend je niet de documenten zelf. Zo voorkom je verschillende versies en dubbele opslag. Zo is informatie beter vindbaar. Wanneer dit niet kan, omdat de ontvanger geen toegang heeft of mag hebben, mag je bijlagen bij uitzondering wel per chat of e-mail versturen.

2.9.7 Gooi binnen vier weken na ontvangst of verzending in Outlook je privé e-mails weg. In Outlook is voor e-mail een vangnetmaatregel ingericht, die e-mails ouder dan vier weken voor een bepaalde periode bewaard. Zie voor meer informatie de interne richtlijnen voor e-mailarchivering op Sharepoint.

2.9.8 Je e-mail (ontvangen en verzonden) in Outlook wordt voor 7 jaar bewaard en daarna automatisch vernietigd. E-mails of berichten die bij een dossier/zaak horen, plaats je in de aangewezen beheeromgeving. Als je niet weet hoe of waar dat moet: raadpleeg je dan je IPM-team.

2.9.9 Voor sleutelfuncties, en de functionele e-mailboxen die horen bij sleutelfuncties, geldt een andere bewaartermijn in Outlook, waarbij de e-mail voor 10 jaar wordt bewaard binnen de Gemeente Utrecht en daarna (voor eeuwig) wordt overgebracht naar Het Utrechts Archief. Sleutelfuncties worden hier apart over geïnformeerd door hun recordmanager en IPM-team.

2.9.10 E-mails en berichten kunnen op grond van de Wet open overheid (Woo) worden opgevraagd door een verzoeker. Een medewerker die over de gevraagde documenten beschikt is verantwoordelijk dat deze beschikbaar worden gesteld bij de aangewezen behandelaar van het Woo-verzoek. De medewerker volgt eventuele instructies van deze behandelaar op, zoals over aanlevertermijnen zodat wettelijke beslistermijn zoveel mogelijk worden gehaald. Het voldoen aan een Woo verzoek is verplicht.

2.9.11 De map verwijderde items in Outlook wordt dagelijks automatisch geleegd. Alle e-mails in die map zijn dan permanent verwijderd.

2.10 Social media

2.10.1 Voor het gebruik van social media, zowel privé áls bedrijfsmatig, gelden de volgende richtlijnen:

- Het gebruik van sociale media op de werkvloer is gebaseerd op gezond verstand, en de normen en waarden die gelden binnen onze organisatie.
- Het privégebruik van sociale media voor privédoeleinden is toegestaan, mits dit beperkt blijft en de uitvoering van werkzaamheden niet belemmert.
- Besef bij het gebruik van sociale media dat alles wat je online zet openbaar is. Ga ervan uit dat sociale media net zo betrouwbaar zijn als een publieke bijeenkomst.
- Bespreek geen vertrouwelijke zaken en verstuur geen vertrouwelijke stukken via sociale media.
- Als jouw profiel aangeeft dat je voor onze organisatie werkt, neem dan ook op dat de berichten die je verstuurt op persoonlijke titel worden geschreven.
- Wees beleefd en respecteer privacy! Als ambassadeur van de organisatie behandel je je gesprekspartner met respect. Je plaatst geen foto’s van collega’s of klanten online zonder hun toestemming. Plaats geen privégegevens online en wees terughoudend in het noemen van namen. De gedragsregels van onze organisatie zijn ook online van toepassing.
- Besef dat ongepaste reacties: a. (de reputatie van) de organisatie kunnen schaden, b. (de reputatie van) jezelf kunnen schaden. Denk dus twee keer na voor je iets plaatst. Realiseer je dat online bijdragen altijd vindbaar blijven.

- Naast de richtlijnen zijn er ook vijf adviezen en zijn er in de vorm van een social media code drie vragen die je jezelf kan stellen als je iets wilt plaatsen of ergens op wilt reageren.

2.10.2 Zakelijke communicatie via social media valt onder de Wet open overheid (Woo) en de Archiefwet (zie ook 3.3.1). Aan publicaties en communicatie via sociale mediakanalen namens de gemeente richting burgers, bedrijven of instellingen kunnen rechten ontleend worden. Sociale mediakanalen zijn geen archiefomgeving, omdat er specifieke eisen aan de inrichting daarvan worden gesteld. Bewaar informatie/documenten bij het (zaak)dossier waar deze bij horen in een omgeving die wel voldoet aan de eisen of creëer een (zaak)dossier op de correcte wijze in zo'n omgeving. Als je niet weet hoe of waar dat moet: raadpleeg dan jouw IPM-team.

3 Apparatuur en gegevens

3.1 Gebruik van apparatuur

3.1.1 In sommige situaties verzorgt de gemeente apparatuur voor haar medewerkers, zoals laptops of telefoons. Maak voor zakelijke doeleinden gebruik van deze uitgereikte apparatuur. Bij uitzondering mag eigen apparatuur gebruikt worden, zolang je werkt binnen de gemeentelijke digitale werkplek. Dit vergroot de kans dat je op een standaard en veilige wijze werkt en dat je informatie op beheerde omgevingen staat. Leen (mobiele) apparatuur van de gemeente niet uit. Dit geldt in zakelijke omgeving bijvoorbeeld voor het uitlenen van je laptop aan collega's, maar ook in privé-omgeving aan bijvoorbeeld je kinderen.

3.1.2 Realiseer je dat het zakelijk gebruik van apparatuur zoals laptops of telefoons (zakelijk en privé apparatuur) onder de Wet open overheid (Woo) en de Archiefwet kan vallen (zie 3.3.1). Het kan daarom voorkomen dat je wordt verzocht om informatie, zoals documenten of gesprekken, in de juiste beheeromgeving op te slaan en/of aan te leveren. Je bent verplicht om hieraan mee te werken.

3.1.3 Wanneer, op apparatuur van de gemeente of eigen apparatuur die je zakelijk gebruikt, wordt aangegeven dat (beveiligings)updates beschikbaar zijn: installeer deze het liefst direct, maar anders bij de eerstvolgende mogelijkheid. Dit geldt met name voor updates van het besturingssysteem (zoals Windows, OSX, Android of iOS) of van beveiligingssoftware zoals een virusscanner.

3.1.4 Gebruik de kabels en andere randapparatuur (zoals als webcams of muizen) van de gemeente. Raadpleeg het serviceplein bij twijfel over de betrouwbaarheid van je zelf gekochte kabels of randapparatuur.

3.1.5 Beveilig de apparatuur die je thuis (of elders) gebruikt om op afstand te kunnen werken. Stel sterke, persoonlijke wachtwoorden in op apparatuur zoals je (WiFi)-netwerk en voer updates door als deze beschikbaar zijn.

3.1.6 Op je mobiele telefoon kan je de app Bedrijfsportal installeren waarmee je onder andere toegang krijgt tot je zakelijke e-mail. Om ervoor te zorgen dat dit veilig gebeurt, zal de app een aparte werkomgeving aanmaken in je telefoon, gescheiden van eventuele persoonlijke apps. Binnen deze werkomgeving heeft de gemeente bepaalde mogelijkheden voor het beheer hiervan, waaronder beveiliging en monitoring (zie 5.1). Lees de handleiding Bedrijfsportal op Sharepoint voor meer details over Bedrijfsportal.

3.1.7 Lever apparatuur van de gemeente na de periode van gebruik altijd in, bijvoorbeeld wanneer je uit dienst gaat of wanneer de apparatuur vervangen moet worden.

3.1.8 Je zakelijke laptop is alleen bedoeld voor zakelijke doeleinden. Je kan daarom zelf geen applicaties hierop installeren.

3.1.9 We werken digitaal. Print alleen als het echt noodzakelijk is en let er daarbij op dat er geen vertrouwelijke documenten bij de printer blijven liggen.

3.1.10 Laat de laptop niet onbeheerd achter in publieke ruimtes. Als je het Stadskantoor of een andere gemeentelocatie verlaat dan neem je de laptop mee of berg je de laptop op in een afsluitbare kast of ruimte.

3.1.11 Meld verlies of diefstal van apparatuur telefonisch bij het Serviceplein (030 -2861010) zodat de toegang tot gemeentelijke netwerken geblokkeerd kan worden. Volg verder de instructies zoals ze op Sharepoint zijn opgenomen.

3.2 Gegevens inzien en maken

3.2.1 Alle gegevens waarmee je werkt, los van of je deze zelf creëert, verzamelt of ontvangt, zijn eigendom van de gemeente en niet van jezelf. De gemeente moet verantwoording afleggen over haar handelen aan de inwoners (Wet open overheid verzoeken), het bestuur, haar managers en aan directe collega's. Daarom moeten wij zorgvuldig omgaan met onze gegevens. Dat geldt ook voor gegevens op privé-apparatuur. Lees in dit kader ook de gouden regels voor informatiebeheer.

3.2.2 Bij je indiensttreding heb je een geheimhoudingsovereenkomst getekend. Wanneer je gegevens zakelijk verwerkt (zoals het inzien, bewerken of verspreiden hiervan) heb je een geheimhoudingsplicht.

3.2.3 Ieder team heeft werkafspraken over het ophalen en opslaan van informatie. Vraag je leidinggevende en je IPM-team hiernaar. Zijn deze afspraken er niet, maak deze dan samen met je team en schakel het IPM-team in voor hulp en advies.

3.2.4 Als je een document (of spreadsheet of presentatie) maakt, is naast de inhoud ook een aantal gegevens belangrijk. Noteer de verantwoordelijke afdeling/auteur en noteer of het een concept is of een vastgestelde versie. Werk hiervoor bijvoorbeeld met versienummers.

3.2.5 Wanneer je informatie uit een andere bron in je document kopieert, vermeld dan een duidelijke referentie naar de bron. Maak bijvoorbeeld gebruik van de beeldbank om oneigenlijk gebruik van intellectueel eigendrom te voorkomen. Gebruik, zonder voorafgaande toestemming, geen gegevens uit een bron die beschermd wordt door intellectueel eigendomsrecht. Vraag, bij twijfel over intellectuele eigendomsrechten, om advies bij Juridische Zaken.

3.2.6 Maak zo weinig mogelijk digitale kopieën van gegevens. Hoe meer kopieën ontstaan, hoe moeilijker het wordt om bij te houden waar deze opgeslagen bestaan, deze actueel te houden en ongewenste verspreiding te voorkomen. Verwijs in plaats daarvan zoveel mogelijk met koppelingen naar het originele bestand.

3.2.7 Gebruik alleen applicaties die standaard op zakelijke apparatuur of in de werkomgeving staan geïnstalleerd, die je aan kan vragen via het Serviceportaal, of waarvan op sharepoint is aangegeven dat ze zijn toegestaan. Het gebruik van gratis (web)apps (bijvoorbeeld voor online samenwerking of bestandsuitwisseling) is niet toegestaan voor zakelijk gebruik: de gemeente kan hiervoor verantwoordelijk worden gehouden. Daarnaast weet je niet zeker of gegevens veilig en privacybewust worden verwerkt.

3.2.8 Maak je iets om te publiceren? Houd dan altijd rekening met wetten rondom digitale toegankelijkheid, zodat de informatie ook door bijvoorbeeld blinden of slechthorenden te raadplegen is. Zie de pagina Digitale toegankelijkheid voor meer informatie.

3.3 Gegevens bewaren, overdragen en vernietigen

3.3.1 Bewaar alle relevante gegevens waar je mee werkt op de plek die daarvoor bestemd is. Vraag je leidinggevende of je IPM-team om advies als de opslaglocatie niet duidelijk is. Met het bewaren van gegevens voldoen we aan onze wettelijke verplichting voor een transparante overheid: Wet open overheid (Woo) en de Archiefwet. Meer informatie over Woo vind je terug op Sharepoint.

3.3.2 Wij werken zoveel als mogelijk digitaal, maar gebruik de speciale papiercontainers op onze kantoorlocaties voor het veilig vernietigen van vertrouwelijke papieren.

3.3.3 Standaard maken we gebruik van MS Teams en het Zaaksysteem. Leg daarom geen persoonlijk archief aan, zoals in je werkomgeving, e-mailbox, harde schijf of mobiel. Persoonlijke domeinen zijn niet bedoeld voor het lange termijn opslaan of archiveren van bedrijfsgegevens.

3.3.4 Sla geen zakelijke gegevens op, op mobiele datadragers zoals USB-sticks. Uitzondering hierop is het opslaan van zakelijke contactgegevens op je telefoon. Let op dat bij belangrijke besluiten deze informatie landt in de aangewezen beheeromgeving.

3.3.5 Verwijder niet zomaar gegevens waaraan, direct of indirect, rechten en/of plichten te ontlenen zijn. Doe dit alleen in overleg met jouw recordmanager zodat die gegevens alleen worden verwijderd volgens de officiële vernietigingsprocedure van de gemeente Utrecht. Uitzondering hierop zijn kopieën.

3.3.6 Als informatie (zoals e-mails en berichten) wordt gevraagd onder de Wet open overheid (Woo) dan mag de medewerker om wiens e-mailbox het gaat of op wiens mobiel de berichten staan geen mails of berichten verwijderen.

3.4 Persoonsgegevens

3.4.1 Wees zorgvuldig met persoonsgegevens: dat is persoonlijke informatie of informatie die aan een specifieke persoon kan worden gerelateerd.

3.4.2 Gebruik in je werk niet meer persoonsgegevens dan noodzakelijk om dit uit te voeren.

3.4.3 Deel persoonsgegevens alleen met partijen die noodzakelijk zijn voor de uitvoering van je taken en waar is vastgesteld dat dit is toegestaan.

3.4.4 Deel geen persoonsgegevens, zoals adres of privé-telefoonnummer, als je niet zeker weet of je ze mag delen. Bespreek in dat geval eerst met een collega's of met je DISO of persoonsgegevens wel gedeeld mogen worden.

3.4.5 Verstuur een verzameling van persoonsgegevens, zoals een lijst met namen en functies, nooit via social media of een standaard e-mailbericht. Als per e-mail toch dergelijke gegevens moeten worden uitgewisseld, maak dan gebruik van extra beveiligde e-mail (zie 2.9.3). Dit geldt voor zowel interne als externe e-mail.

3.4.6 Sla nooit persoonsgegevens op, op plekken die niet formeel zijn goedgekeurd, zoals in eigen apps of online opslagdiensten.

3.4.7 Gaat er iets mis en zijn er persoonsgegevens bij betrokken? Bijvoorbeeld het verlies van een USB-stick of een brief die naar een verkeerd adres is verstuurd, zie dan hierna bij het melden van datalekken (4.1).

3.4.8 Voor veel processen waarin (gevoelige) persoonsgegevens van inwoners maar ook van medewerkers worden verwerkt, is risicoanalyse (DPIA) opgesteld. Dit is een analyse van de privacyaspecten van een proces, wat je handvatten kan geven in de uitvoering hiervan.

3.4.9 Heb je privacy-gerelateerde vragen? Bijvoorbeeld over het verwerken van persoonsgegevens of het delen ervan. Hiervoor kan je terecht bij de DISO van je organisatieonderdeel.

4 Incidenten

Het is belangrijk om alle (mogelijke) incidenten zo snel maar in ieder geval binnen 4 uur te melden. Door dit te doen kan snel bepaald worden wat er moet gebeuren om het incident op te lossen en eventuele (vervolg) schade te beperken of voorkomen. Ook kan hierdoor worden voldaan aan de wettelijke eisen die bijvoorbeeld gelden voor het melden van een datalek bij de Autoriteit Persoonsgegevens. De regels en afspraken over incidenten worden hierna genoemd en toegelicht.

4.1 Beveiligingsincidenten en datalekken

4.1.1 Een beveiligingsincident is een lek in de beveiliging van apparatuur, software of de kantoorlocatie.

4.1.2 Als medewerker van de gemeente moet je alle (mogelijke) beveiligingsincidenten of datalekken melden via de servicedesk, aan je leidinggevende of de DISO van jouw organisatieonderdeel. Voorbeelden van beveiligingsincidenten zijn:

- Diefstal/verlies van een laptop, USB-stick of mobiele telefoon.
- Een gestolen privé apparaat waar zakelijke gegevens op staan.
- Onjuiste adressering van post.
- Een e-mail met persoonsgegevens die onbedoeld naar een persoon wordt verstuurd.
- Ongeautoriseerde toegang tot vertrouwelijke gegevens.
- Phishing e-mails of -telefoontjes.

4.1.3 Als er bij bovenstaande voorbeelden persoonsgegevens betrokken zijn kan er sprake zijn van een datalek. Bij een datalek komen persoonsgegevens terecht bij iemand die geen toegang tot die gegevens mag hebben, of gaan gegevens verloren zonder dat een back-up van de gegevens bestaat.

4.1.4 Meld ook ‘kleine’ beveiligingsincidenten of datalekken, ook wanneer je denkt dat de impact niet zo groot is.

4.1.5 Stel het melden van een beveiligingsincident of datalek niet uit, maar doe dit gelijk of in ieder geval binnen vier werkuur. De gemeente is wettelijk verplicht om zo snel mogelijk op een datalek te reageren en (indien nodig) de autoriteiten en hiervan op de hoogte te stellen.

4.1.6 Je kan voor het melden ook gebruik maken van het meldingsformulier Beveiligings- of datalek melden op utrecht.nl. Indien gewenst kan je dit anoniem doen.

4.1.7 Heb je een (potentieel) beveiligingsincident gevonden? Deel dan je bevinding niet met anderen, in ieder geval niet totdat het lek is hersteld. Maak ook geen actief misbruik van het beveiligingsincident.

5 Toezicht

5.1 Controle

5.1.1 De gemeente heeft de verplichting en het belang om haar netwerk en systemen en de (persoons)gegevens die daarbinnen verwerkt worden te beschermen en beveiligen. Onderdeel van het beschermen en beveiligen is controle (het loggen en monitoren) van het netwerk en de systemen waar we binnen de gemeente mee werken. De log-gegevens die worden verzameld kunnen persoonsgegevens van medewerkers bevatten. Deze gegevens van medewerkers zijn niet het primaire doel van de controles en worden tot een minimum beperkt.

5.1.2 Om de privacy van medewerkers bij de hiervoor genoemde controles te waarborgen en te beschermen wordt bij de inzet van controles een risicoanalyse uitgevoerd en zo nodig een DPIA (Data Protection Impact Assessment) uitgevoerd. Waar van toepassing wordt de COR om instemming gevraagd.

5.1.3 De controle op het gebruik van automatiseringsmiddelen en gegevens zal overeenkomstig dit protocol en het Onderzoeksprotocol integriteitsschendingen en misstanden uitgevoerd worden.

5.1.4 Als zich situaties voordoen waarin deze regelingen niet voorzien, zal in overeenstemming met de wet- en regelgeving waaronder: het Handboek Utrechts Personeel, de CAO gemeenten en de Algemene Verordening Gegevensbescherming (AVG) worden gehandeld.

5.2 Organisatorische / algemene controle

5.2.1 Er worden verschillende soorten controles uitgevoerd. Mogelijke controles zijn:

- Geautomatiseerde controle op virussen en schadelijke programma's in het kader van systeem- en netwerkbeveiliging.
- Controle om te borgen dat er voldoende systeemcapaciteit is. Dit gebeurt door het bekijken van activiteiten op het netwerk en online en het analyseren van gebruikerspatronen.
- Als er een vermoeden bestaat dat vertrouwelijke informatie wordt gelekt.

5.2.2 Organisatorische en algemene controles kunnen worden gespecificeerd tot afdelingsniveau en individueel niveau als de controle hiertoe aanleiding geeft. Bijvoorbeeld bij zeer grote aantallen e-mails, excessieve stijging van bezoek aan niet zakelijke internetsites enz.

5.2.3 Er is een overzicht beschikbaar van de controles waar persoonsgegevens van medewerkers in betrokken zijn.

5.3 Individuele controle

5.3.1 Als er op basis van een organisatorische en/of algemene controle een redelijk vermoeden van een integriteitsschending door een medewerker ontstaat, zal op basis van het Onderzoeksprotocol integriteitsschendingen en misstanden nader onderzoek worden verricht.

5.3.2 Het gebruik van automatiseringsmiddelen en gegevens door een individuele medewerker kan gecontroleerd in het kader van een onderzoek zoals beschreven in het Onderzoeksprotocol integriteitsschendingen en misstanden.

5.3.3 Als bij een onderzoek integriteitsschending is vastgesteld dat er sprake is van handelen in strijd met de bepalingen in dit protocol kan dit leiden tot arbeidsrechtelijke consequenties

5.4 Rechten van medewerkers

5.4.1 De wettelijke richtlijnen met betrekking tot de privacy van medewerkers zijn onverminderd van toepassing. De privacyrechten van medewerkers staan in hoofdstuk III van de AVG, nader uitgewerkt in de gemeentelijke privacyverordening. De Autoriteit Persoonsgegevens geeft hier een duidelijke toelichting op.

5.4.2 De verplichtingen uit het protocol en de rechten van de medewerker, voor zover van toepassing, blijven ook na uit dienst treden bestaan. Een voorbeeld hiervan is geheimhouding.

5.4.3 Heb je vragen over je rechten als medewerker? Stel deze aan je leidinggevende of via het Serviceportaal HRM.