5.2 Gedragscode voor het gebruik van ICT diensten en ICT middelen

1. Algemeen/toepassingsbereik

1.1 Deze regeling geeft de wijze aan waarop binnen de organisatie van ENGIE wordt omgegaan met het gebruik van ICT diensten en ICT middelen. Deze regeling omvat gedragsregels ten aanzien van een verantwoord gebruik van ICT diensten en ICT middelen en regels over de wijze waarop controle op dit gebruik plaats vindt.

Onder '**ICT middelen'** wordt verstaan: Alle middelen die een rol vervullen in informatie- en communicatieprocessen. Het gaat hierbij onder meer om PC's, (mobiele) telefoons, printers, informatiedragers, kopieerapparatuur, scanners, internettoegang, e-mail, systeemsoftware en applicaties.

Onder **'ICT diensten'** wordt verstaan: Het geheel aan ICT infrastructuur, Apps en bedrijfsapplicaties welke beschikbaar gesteld worden als dienst zodat uitvoering gegeven kan worden aan de bedrijfsprocessen van ENGIE.

Onder **ENGIE** wordt verstaan de naamloze vennootschap ENGIE Services Nederland N.V., de naamloze vennootschap ENGIE Energie Nederland N.V. en alle aan deze beide bedrijven gelieerde vennootschappen (in deze gedragscode ook wel "werkmaatschappijen" genoemd).

Deze gedragscode geldt voor een ieder die werkzaamheden voor ENGIE verricht op basis van een overeenkomst met ENGIE. Onder werknemer wordt ook de tijdelijke werknemer verstaan.

1.2 De controle op het gebruik van ICT diensten en ICT middelen en het verwerken van persoonsgegevens in dat kader vindt plaats met als doel:

- het bewaken van de veiligheid en integriteit van de ICT infrastructuur. Dit omvat onder meer het voorkomen van de verspreiding van virussen of andere data die een bedreiging voor de ICT infrastructuur vormen;
- gegevens te verzamelen die de kosten- en capaciteitsplanning faciliteren;
- gegevens te verzamelen waarmee de ICT infrastructuur, ICT diensten en ICT middelen veiliger, effectiever, efficiënter en gebruikersvriendelijker kunnen worden ingericht;
- het voorkomen van misbruik van ICT diensten en ICT middelen;
- het beperken van overmatig privégebruik van ICT diensten en ICT middelen;
- het voorkomen van de bezichtiging van websites met pornografische, racistische of anderszins discriminerende en seksueel intimiderende inhoud of andere inhoud die in strijd is met de nationale of internationale wetgeving;
- het voorkomen van uploading, downloading en verspreiding van data, inclusief maar niet beperkt tot e-mail en bestanden, met pornografische, racistische en seksueel intimiderende inhoud of andere inhoud die in strijd is met de nationale of internationale wetgeving, en
- het voorkomen van het uitlekken van bedrijfsgevoelige informatie.

1.3 De controle op het gebruik van ICT diensten en ICT middelen zal overeenkomstig deze gedragscode uitgevoerd worden. Indien er zich situaties voordoen waarin deze regeling niet voorziet, zal conform het algemeen arbeidsrechtelijk kader en de Algemene Verordening Gegevensbescherming (AVG) en in overleg met de (centrale) ondernemingsraad gehandeld worden.

1.4 Gestreefd wordt naar een goede balans tussen controle op verantwoord gebruik van ICT diensten en ICT middelen en bescherming van de privacy van werknemers op de werkplek.

2. Algemene uitgangspunten voor gebruik van ICT diensten en ICT middelen

2.1 Gebruik van ICT diensten en ICT middelen moet altijd plaatsvinden in overeenstemming met nationale en internationale regelgeving. De gebruikelijke gedragsregels, zoals de regels die thans gelden voor het ondertekenen van schriftelijke correspondentie, het vertegenwoordigen van ondernemingen binnen ENGIE en voor het verzenden van post (zoals correct taalgebruik en huisstijl) zijn onverkort van toepassing op het gebruik van ICT diensten en ICT middelen. Algemene gebruiksregels, in overeenstemming met algemeen geaccepteerde normen en waarden en door de wet bepaald, gelden onverkort voor het gebruik van ICT diensten en ICT middelen.

Werknemers hebben ICT diensten en ICT middelen ter beschikking gekregen voor zakelijk gebruik. Het gebruik van ICT diensten en ICT middelen zowel intern als extern voor persoonlijke doeleinden zijn in beperkte mate toegestaan voor zover dit niet storend is voor de dagelijkse werkzaamheden en dit geen onredelijke belasting van de ICT infrastructuur veroorzaakt. Dit met in achtneming dat privé gebruik van het ENGIE e-mailadres zoveel als mogelijk voorkomen wordt.

ENGIE geeft haar werkplek een steeds meer open karakter. Hierbij krijgen werknemers meer en meer mogelijkheden deze te personaliseren door instellingen aan te passen en zelf programmatuur toe te voegen. Deze vrijheid vraagt van de werknemer meer discipline en terughoudendheid om te voorkomen dat noodzakelijke toepassingen niet meer (goed) functioneren. De werknemer dient zich ervan bewust te zijn dat deze ‘vrijheden’ ook risico’s met zich mee brengen. Indien dit in de praktijk tot ongewenste situaties leidt, kunnen bepaalde mogelijkheden terug gedraaid worden.

Licenties voor door ENGIE geleverde programmatuur worden door ENGIE verzorgd. De werknemer heeft met de komst van een nieuw werkplek concept de mogelijkheid zelf software te installeren op het ENGIE ICT middel (laptop e.d.). De werknemer die niet door ENGIE geleverde programmatuur installeert is er zelf voor verantwoordelijk om te voldoen aan de voorwaarden van de betreffende fabrikant of leverancier aangaande het productgebruik. En, indien van toepassing, dient de werknemer er zelf voor zorg te dragen dat eventueel noodzakelijke licenties inclusief betaling daarvan op persoonlijke titel verzorgd wordt.

ENGIE baseert haar werkplekdiensten op de Microsoft Cloud diensten. Hierbij krijgt de werknemer zowel privé als zakelijk de mogelijkheid gebruik te maken van de Microsoft Cloud diensten. De werknemer dient zich te realiseren dat er informatie over het gebruik geregistreerd wordt bij Microsoft en beschikbaar is binnen ENGIE. Het gebruiksrecht vervalt bij uitdiensttreding.

2.2 Niet elke gebruiker heeft per definitie de beschikking over ICT diensten en ICT middelen. Indien voor de uitoefening van zijn/haar werkzaamheden toegang tot ICT diensten en ICT middelen noodzakelijk is, zal deze werknemer hiertoe toegang krijgen. Of toegang zal worden verstrekt is ter beoordeling van de direct leidinggevende en het management van ENGIE en/of de betreffende werkmaatschappij. ENGIE kan het recht tot gebruik van (een deel van) de ICT diensten en ICT middelen toestaan, maar ook weer intrekken. De omvang van het gebruik van ICT diensten en ICT middelen is afhankelijk van de verschafte rechten.

2.3 Gebruiker identificatie (inlognaam) en wachtwoorden zijn persoonsgebonden. Deze mogen niet met anderen worden gedeeld, tenzij dit vereist is voor de uitvoering van de werkzaamheden in overeenstemming met de functieomschrijving, en pas na vooraf verkregen schriftelijke toestemming van de direct leidinggevende.

2.4 Vertrouwelijke gegevens en bedrijfsgevoelige informatie (inclusief maar niet beperkt tot persoons-, klant- en leverancier gegevens) moeten altijd vertrouwelijk worden behandeld en mogen niet zonder toestemming buiten de organisatie van ENGIE gebracht worden.

2.5 In het bijzonder in publieke ruimten dient een werknemer zich bewust te zijn van de risico's die verbonden zijn aan het gebruik van publiek toegankelijke Wi-Fi hotspots.

2.6 Een werknemer dient bij het verlaten van de werkplek alle aan hem/haar ter beschikking gestelde ICT diensten en ICT middelen te blokkeren ter voorkoming van onbevoegd gebruik. Hierbij zal ook de informatie op het scherm afgeschermd worden zodat geen (vertrouwelijke) data zichtbaar blijft. Een automatische screensaver treedt in werking indien gedurende een bepaalde tijd geen activiteit is waargenomen, gevolgd door het blokkeren van de betreffende ICT diensten en ICT middelen.

2.7 Het is niet toegestaan inkomend dataverkeer te genereren door bijvoorbeeld deel te nemen aan niet-werk gerelateerde informatie-, muziek-, video- of vergelijkbare (streaming)diensten welke een onredelijke belasting kunnen veroorzaken van de ICT infrastructuur ten behoeve van bedrijfsmatige diensten.

3. Internet

3.1 Onverminderd het elders in deze gedragscode bepaalde, is het de werknemer niet toegestaan om op of via het internet:

- bewust websites te bezoeken en/of te bezichtigen die beledigend en/of aanstootgevend kunnen zijn, inclusief maar niet beperkt tot websites die pornografisch of anderszins seksueel getint materiaal bevatten, dan wel racistisch of discriminerend materiaal bevatten;
- bestanden te downloaden die beledigend en/of aanstootgevend kunnen zijn en/of bestanden waarvoor geen licentieovereenkomst bestaat, inclusief maar niet beperkt tot bestanden die pornografisch of anderszins seksueel getint materiaal bevatten, dan wel racistisch of discriminerend materiaal bevatten;
- bestanden te downloaden die auteursrechtelijk beschermde werken bevatten, en waarvoor de maker/rechthebbende niet expliciet toestemming tot downloaden en gebruik verleent;
- deel te nemen aan kansspelen in strijd met geldende wet- en regelgeving;
- illegale software te downloaden dan wel te installeren of anderszins te gebruiken;
- zich voor te doen als een andere persoon;
- zich ongeoorloofd toegang te verschaffen tot niet-openbare bronnen op het internet;
- opzettelijk informatie waartoe via het internet toegang is verkregen zonder toestemming te veranderen of te vernietigen;
- strafbare feiten te plegen of anderszins in strijd met de wet of onethisch te handelen;
- opzettelijk ENGIE bedrijfsinformatie d.m.v. internet te openbaren.

3.2 Gedragsregels voor online media (LinkedIn, Twitter, Facebook, Yammer, What's App. ed.)

Wees bij het gebruik van social media altijd bewust van het bedrijfsbelang en het imago van ENGIE. Werknemers zijn verplicht zich te houden aan de gepubliceerde richtlijnen voor het gebruik van social media door werknemers van ENGIE. Voor de datum van uitdiensttreding dient de werknemer zelfstandig en ongevraagd zichzelf te verwijderen uit applicaties of groepen, zoals bijvoorbeeld een What's App groep met collega's, welke een overwegend zakelijk karakter hebben, vertrouwelijke informatie bevat en werknemer weet of zou moeten vermoeden dat deze niet door een ICT afdeling beheerd worden.

4. E-mail

4.1 Onverminderd het elders in deze gedragscode bepaalde moet het versturen van e-mail minimaal voldoen aan de volgende voorwaarden:

- het verzenden van e-mail die wettelijk beschermde en/of vertrouwelijke informatie bevat, mag uitsluitend na vooraf gegeven schriftelijke toestemming door de auteur van de informatie, worden verstuurd. In dergelijke gevallen zal de exclusiviteit van e-mail door middel van aanvullende maatregelen moeten worden gegarandeerd en zal het moeten worden uitgevoerd conform de genoemde uitgangspunten;

- het verzenden van e-mail aan niet meer geadresseerden dan noodzakelijk en verwacht geen reactie van iemand naar wie u een kopie (cc) stuurt;
- gebruik uitsluitend mailinglijsten (een mailinglijst is een soort abonnement waarbij men over een bepaald onderwerp automatisch allerlei e-mail berichten toegestuurd krijgt) als dit voor het werk noodzakelijk is;
- het conform de ENGIE richtlijnen ondertekenen en eventueel versleutelen van mails als de inhoud conform de bedrijfsrichtlijnen dit vereist;
- gebruik zoveel als mogelijk door ENGIE beschikbaar gestelde cloud media als Office 365 voor het uitwisselen van grote bestanden in plaats van deze via e-mail bijlagen te verspreiden;
- sluit een e-mail af met de handtekening die voldoet aan de ENGIE huisstijl en die elektronisch en geautomatiseerd beschikbaar gesteld wordt. Slechts in uitzonderingssituaties kunnen hierin kleine aanpassingen gemaakt worden door hiervoor een kopie handtekening te maken (denk bv. aan de toevoeging “Niet werkzaam op vrijdag”);
- wanneer werknemers hun e-mail langer dan 5 werkdagen niet (kunnen) inzien, zijn zij verplicht de ontvangen e-mails automatisch te laten beantwoorden door middel van de afwezigheidmelder van de in gebruik zijnde e-mail applicatie; en
- elke e-mail die verzonden wordt naar een extern adres (buiten ENGIE), zal automatisch door de centrale e-mailserver van een disclaimer worden voorzien.

4.2 Onverminderd het elders in deze gedragscode bepaalde is het in het bijzonder niet toegestaan om door middel van e-mail:

- berichten anoniem of onder een fictieve naam te versturen;
- dreigende, beledigende, aanstootgevende, seksueel getinte of intimiderende, racistische, discriminerende dan wel zgn. ketting e-mail berichten te versturen of te ontvangen;
- iemand op een hinderlijke wijze ongewenste berichten te sturen; en
- berichtenverkeer te genereren waardoor ENGIE redelijkerwijs schade kan worden toegebracht, waaronder wordt begrepen de aantasting van de goede naam.

Als de werknemer een dergelijk bericht ontvangt dient hij onmiddellijk zijn direct leidinggevende hierover in te lichten.

4.3 Het is niet toegestaan om een e-mail naar nagenoeg alle medewerkers van meer vestigingen dan die vestigingen behorende tot een bepaalde werkmaatschappij, te versturen, tenzij hiervoor schriftelijke toestemming van een bestuurder van de betreffende werkmaatschappij is verkregen of het versturen van dergelijke communicatie onderdeel is van de functie van betreffende werknemer.

5. Data opslag

Onverminderd het elders in deze gedragscode bepaalde is voor het opslaan van data het volgende van toepassing:

- opslaan van ENGIE data op externe media, zoals een USB disk of flash drive, is alleen toegestaan indien deze versleuteld wordt. De werknemer is hierbij verantwoordelijk voor het veilig omgaan met en bewaren van wachtwoorden en herstelsleutels (recovery keys). Interne media in ENGIE devices, zoals een harddisk of Solid State Disk (SSD) in een laptop, wordt standaard vanuit ICT versleuteld met inbegrip van het veiligstellen van de herstelsleutels.
- voor zakelijke data met een persoonlijk karakter biedt ENGIE haar werknemers met een Windows device Cloud opslag aan (Microsoft OneDrive als onderdeel van de cloud dienst Office 365) ter vervanging van de home folder (‘Mijn documenten’). Het eventueel delen met anderen van deze data (in de cloud) is een verantwoordelijkheid van de werknemer. Bij uitdiensttreding dient de werknemer nog relevante data tijdig veilig te stellen. Na het blokkeren/opheffen van het inlog account kan niemand hier meer bij, ook de afdeling ICT niet.
- bestanden opgeslagen in de home folder (‘Mijn documenten’) en netwerk fileshares (zoals bv. g:, i: en u:) worden door de ICT afdeling centraal veilig gesteld. Bestanden opgeslagen in OneDrive worden door Microsoft in de cloud veilig gesteld. Werknemers dienen geen ENGIE data op lokale disks (zoals c: en d:) op te slaan daar deze niet veilig gesteld worden en verloren kunnen gaan

bij verlies, diefstal en defecten. PS: Lokale opslaglocaties ‘OneDrive - ENGIE’ en ‘ENGIE’ bevatten gesynchroniseerde data uit de cloud OneDrive respectievelijk cloud SharePoint sites en worden dus in de cloud veilig gesteld.

6. Controle

6.1 Controle op het gebruik van ICT diensten en ICT middelen vindt slechts plaats in het kader van de in artikel 1.2 van deze regeling genoemde doelen.

6.2 Met betrekking tot opslag media verstrekt door ENGIE aan medewerkers, vindt controle plaats van de hoeveelheid en typen bestanden ten behoeve van het waarborgen van de continuïteit van de ICT dienstverlening.

6.3 Alle verzonden en ontvangen data van ICT diensten en ICT middelen wordt op geautomatiseerde wijze gecontroleerd op virussen of vergelijkbare bestanden die een bedreiging vormen voor de veiligheid en integriteit van ENGIE, haar werknemers of de ICT infrastructuur, alsmede op inhoud of bijlagen die duiden op strijd met deze gedragscode. Hiervoor wordt onder andere content filtering software gebruikt. Indien een dergelijke bedreiging wordt geconstateerd, dan zal de data automatisch geblokkeerd worden. De werknemer wordt hiervan in kennis gesteld bij verzending of ontvangst daarvan. Mocht de werknemer onverhoopt toch dergelijke data ontvangen, dan dient hij onmiddellijk zijn direct leidinggevende hiervan in kennis te stellen.

6.4 Een controle op het gebruik van ICT diensten en ICT middelen die gericht is op een bepaalde werknemer vindt slechts plaats op basis van zwaarwichtige redenen en na overleg met leidinggevende en/of HR. Tot deze redenen behoort onder meer een concrete verdenking van overtreding van deze gedragscode. Bij een dergelijke controle bestaat de mogelijkheid onder meer uit het openen, bekijken, opslaan en kopiëren van dataverkeer gegenereerd en ontvangen door de werknemer. Dit houdt ook in het openen en lezen van e-mail. ENGIE zal die controle activiteiten ondernemen die in een redelijke verhouding staan tot het belang van de werknemer. Tevens zal ENGIE niet verdergaande controle activiteiten ondernemen dan in het gegeven geval noodzakelijk is. Bij gegronde verdenking van strafbare feiten behoudt ENGIE zich het recht voor ICT diensten en ICT middelen beschikbaar te stellen aan derden in het kader van het doen van aangifte.

6.5 E-mail berichten van OR-leden, bedrijfsartsen en andere medewerkers met een vertrouwensfunctie zijn in beginsel - oftewel voor zover in hoedanigheid van hun functies als OR-lid, bedrijfsarts of andere vertrouwensfunctie - uitgesloten van gerichte controle. Dit geldt niet voor de controle op de veiligheid van het berichtenverkeer.

6.6 Persoonsgegevens en loggegevens over gebruik van internet en e-mail worden niet langer bewaard dan noodzakelijk, met een bewaartermijn van maximaal twaalf maanden. Als persoonsgegeven wordt aangemerkt elk gegeven betreffende een geïdentificeerde of identificeerbare persoon.

6.7 Controle vindt in beginsel plaats door het monitoren alsook steekproefsgewijs controleren van het gebruik van ICT diensten en ICT middelen. Een dergelijke controle is gericht op het detecteren van bedreigingen welke de business continuïteit van ENGIE in gevaar kunnen brengen. Hierbij worden gebruiker statistieken gegenereerd, welke niet langer dan twaalf maanden bewaard worden en tot doel hebben de eventuele bron van het risico voor ENGIE te kunnen bepalen, om deze vervolgens te kunnen bestrijden. De bevoegdheid tot het uitvoeren van de controleactiviteiten is belegd bij de afdeling ICT onder de verantwoordelijkheid van de CISO. Deze is verplicht tot geheimhouding omtrent alle gegevens die gegenereerd zijn door de controleactiviteiten.

6.8 De leidinggevende die om zwaarwichtige redenen gerichte controle wil laten uitvoeren op het gebruik van ICT diensten en ICT middelen zal dit schriftelijk melden bij een bestuurder van de betreffende

werkmaatschappij. De bestuurder legt het verzoek ter validatie voor aan de manager (internal) Control ter bewaking van het proces en het minimaliseren van de toegang tot informatie van betrokken medewerkers tot het strikt noodzakelijke. Alleen bij goedkeuring van de Ethics en Compliancy manager en de Data Privacy Manager (DPM) wordt het verzoek voorgelegd aan ICT. ICT doet een laatste finale validatie of alle mandaten aanwezig zijn door zowel CIO als CISO alvorens de toegangsaanvraag tot specifiek de gevraagde informatie uitgevoerd wordt.

De Security Manager ICT rapporteert vervolgens aan de algemeen directeur en de Data Privacy Manager (DPM) over de resultaten van de controle. Buiten deze rapportageverplichting zal op alle betrokken personen een geheimhoudingsplicht rusten.

6.9 Tenslotte wordt het mobiel gebruik financieel opgevolgd. Bij een hoger maandelijks verbruik dan €500,- wordt dit voorgelegd aan direct leidinggevend. Deze bespreekt dit met de betrokken medewerker en als blijkt dat er sprake is van oneigenlijk gebruik wordt HR ingelicht alsmede de directeur van de desbetreffende organisatie.

6.10 Controle gericht op een bepaalde werknemer zal pas plaatsvinden als de Manager (Internal) Control, de Data Privacy Officer en de Ethics en Compliancy Officer schriftelijk akkoord hebben gegeven. Hierna zal dit voorgelegd worden aan ICT waar de CISO alsook de CIO een finaal akkoord moet geven alvorens ICT administrators, die onder een NDA verklaring werken, de gevraagde informatie gaan verzamelen. Standaard is de toegang tot privacy gevoelige informatie geblokkeerd en/of is de privacy gevoelige informatie geanonimiseerd. Een uitzondering hierop vormt de toegang van enkele ICT administrators die de toegang tot de informatie regelen. Alleen in voorkomende casussen wordt dit tijdelijk opgeheven onder de strikte regels van Data Privacy. Alle genomen processtappen inclusief de bijbehorende akkoorden worden vastgelegd, zodat achteraf controle s/ audits uitgevoerd kunnen worden op de uitvoering van het proces.

7. Rechten van de betrokkenen

7.1 ENGIE informeert de werknemers voorafgaand aan de invoering van de regeling over controle op ICT diensten en ICT middelen, omtrent de doeleinden, de aard van de gegevens, de omstandigheden waaronder zij verkregen zijn en de inhoud van deze regeling.

7.2 De werknemer[1] kan zich tot het Data Protection Team van ENGIE richten met het verzoek om een volledig overzicht van zijn verwerkte persoonsgegevens. Het verzoek wordt binnen 30 dagen beantwoord.

7.3 De werknemer[1] kan via het Data Protection Team van ENGIE verzoeken zijn persoonsgegevens te verbeteren, aan te vullen, te verwijderen of af te schermen indien deze feitelijk onjuist zijn, voor het doel onvolledig of niet ter zake dienend, dan wel in strijd met een wettelijk voorschrift worden verwerkt. Het verzoek wordt binnen 30 dagen beantwoord.

7.4 De werknemer[1] kan bij het Data Protection Team van ENGIE verzet aantekenen tegen de verwerking van zijn persoonsgegevens in verband met bijzondere persoonlijke omstandigheden. ENGIE oordeelt binnen 30 dagen na ontvangst van het verzet of dit gerechtvaardigd is. Indien ENGIE het verzet gerechtvaardigd acht, beëindigt deze terstond de verwerking.

8. Toegang tot bestanden in nood of tijdens afwezigheid

In geval van nood en bij afwezigheid van de werknemer kunnen bepaalde documenten benodigd voor de voortgang en uitvoering van de bedrijfsprocessen van ENGIE, niet bereikbaar zijn. In

[1] Werknemers van BU GEN en BU GEM kunnen zich wenden tot de Data Privacy Manager van hun BU.

dergelijke gevallen is het aan de direct leidinggevende om in overleg met HR een verzoek tot toegang in te dienen. Slechts indien betrokkene niet binnen een redelijke termijn bereikt kan worden en inzage kan naar redelijkheid niet langer wachten, kan de direct leidinggevende een procedure tot het verkrijgen van toegang opstarten. Hierbij wordt in overleg met HR het verzoek voorgelegd ter validatie aan de manager (internal) Control ter bewaking van het proces en het minimaliseren van de toegang tot informatie van betrokken medewerkers tot het strikt noodzakelijke. Alleen bij goedkeuring van de Ethics en Compliancy manager en de Data Privacy Manager (DPM) wordt het verzoek voorgelegd aan ICT. ICT doet een finale validatie of alle mandaten aanwezig zijn door zowel CIO als CISO alvorens de toegangsaanvraag tot specifiek de gevraagde informatie uitgevoerd wordt.

9. Diefstal, vermissing en/of schade

Mobiele ICT middelen zijn gevoeliger voor diefstal en beschadiging. Indien u beschikt over mobiele ICT middelen dient u zich aan de volgende regels te houden:

9.1 Mobiele ICT middelen mogen niet onbeheerd achter gelaten worden. Niet binnen kantoor en niet buiten kantoor. Binnen kantoor moeten laptops met een veiligheidskabel aan een bureau o.i.d. vastgemaakt worden (bij verlies van de sleutel dient u contact op te nemen met de afdeling ICT).

9.2 Zowel diefstal, vermissing of beschadiging van mobiele ICT middelen als ook diefstal of vermissing van documenten welke persoonsgegevens bevatten moeten zo snel mogelijk maar uiterlijk binnen 24 uur aan de afdeling ICT en uw direct leidinggevende gemeld worden. U dient bij diefstal of vermissing van mobiele ICT middelen aangifte te doen bij de politie en een kopie van die aangifte in te leveren bij ICT

9.3 Werknemer dient al datgene te doen of na te laten om eventuele gevolgschade van de diefstal of vermissing te voorkomen (bijvoorbeeld het stopzetten van een abonnement bij de provider). Voor zover de afdeling ICT acties in dat kader uitvoert geeft de werknemer hieraan volledige medewerking.

9.4 Bij diefstal, vermissing en/of schade, ontstaan door aantoonbaar nalatig gedrag of opzet van de werknemer, kunnen de kosten die (in-)direct daarvan het gevolg zijn op werknemer worden verhaald, onverminderd het recht van werkgever om de werknemer een disciplinaire maatregel op te leggen, indien het geval daartoe aanleiding geeft.

10. Zorgplicht ENGIE bedrijfsgegevens

Het is en wordt steeds makkelijker informatie te delen. Informatie is steeds eenvoudiger toegankelijk, niet alleen op zakelijke ICT middelen maar ook op privé ICT middelen. ENGIE voorziet zoveel als mogelijk in beveiligingsmaatregelen om de bedrijfsinformatie van ENGIE te beschermen. Dit ontslaat de ENGIE medewerker er niet van om:

10.1. Zorgvuldig en bewust om te gaan met het uitwisselen van bedrijfsinformatie, tussen personen alsook tussen ICT middelen;

10.2. Het niet opslaan / downloaden van bedrijfsinformatie op niet ENGIE ICT middelen, tenzij de informatie of ICT middelen voorzien zijn van door ENGIE aangeboden beveiligingsmiddelen of -technieken, zoals versleuteling van data;

10.3. Bedrijfsgegevens te behandelen in lijn met de beleidsafspraken informatieclassificatie en behandeling bedrijfsinformatie van ENGIE en/of conform de interne ENGIE Data privacy Policy en/of de Algemene Verordening Gegevensbescherming dan wel de algemeen geldende wet- en regelgeving.

11. **Duurzaamheid**

Aangezien duurzaamheid een van de strategische pijlers is van ENGIE, vragen wij medewerkers bij het afsluiten van de werkdag, alle ICT middelen (PC, beeldschermen, etc..) uit te schakelen om zo bij te dragen aan de duurzaamheidsdoelstellingen van ENGIE.

12. Duur en beëindiging

12.1 De ICT middelen worden ter beschikking gesteld zolang naar het oordeel van werkgever het gebruik hiervan zakelijk vereist is. Bij functiewijziging beoordeelt werkgever of daarvan in de nieuwe functie sprake is. Is op enig moment naar het oordeel van de werkgever een of meerdere ICT middelen niet

meer vereist voor een goede invulling van de functie van de werknemer, of als de werknemer –al dan niet tijdelijk– van diens taak is ontheven, bij beëindiging dienstverband of (langdurig) met ziekteverlof is, zal werknemer op eerste verzoek van werkgever, de (het) ICT middel(en) in ordentelijke staat retourneren aan werkgever.

12.2 Indien het ICT middel niet, niet tijdig en/of niet in behoorlijke staat wordt ingeleverd, is werknemer aansprakelijk voor de schade die werkgever hierdoor mocht lijden.

13. Klachtenprocedure

13.1 Indien de werknemer meent benadeeld te zijn in zijn rechten op grond van deze gedragscode, kan hij zich richten tot de ondernemingsraad. De ondernemingsraad stelt vervolgens een beroepscommissie in. De beroepscommissie bestaat uit de manager HR van de vestiging waar de werknemer werkzaam is (in de rol van voorzitter), een lid van de ondernemingsraad, de Data Privacy Manager en de vertrouwenspersoon. De beroepscommissie vormt zich binnen 30 dagen na ontvangst van de klacht een oordeel over de gegrondheid van de klacht en deelt dit schriftelijk mee aan de werknemer. De werknemer en een vertegenwoordiger van de onderneming hebben het recht om hun zienswijze mondeling dan wel schriftelijk toe te lichten. Het oordeel van de beroepscommissie is een bindende uitspraak. De beroepscommissie kan alleen bindende uitspraken doen met betrekking tot de naleving van de gedragscode en de zorgvuldigheid van het onderzoek.

14. Sancties

14.1 Werknemers ten aanzien van wie geconstateerd is dat zij zich niet aan deze regeling houden, worden zo spoedig mogelijk door de leidinggevende op hun gedrag aangesproken.

14.2 Bij handelen in strijd met deze gedragscode, het bedrijfsbelang of de algemeen geldende normen en waarden voor het gebruik van ICT diensten en ICT middelen kan ENGIE maatregelen treffen. De aard van de maatregelen is afhankelijk van de aard en de ernst van de overtreding. Deze maatregelen kunnen disciplinaire en arbeidsrechtelijke maatregelen betreffen, zoals berisping, overplaatsing, schorsing en beëindiging van de arbeidsovereenkomst. (Het treffen van) deze maatregelen la(a)t(en) onverlet het recht van ENGIE om daarnaast volledige schadevergoeding te eisen.

15. Slotbepaling

15.1 Deze gedragscode is tot stand gekomen in overleg met en met instemming van de ondernemingsraad bij besluit van 26 november 2019 en treedt vanaf deze datum in werking.

15.2 Deze gedragscode laat elke uit wet, collectieve arbeidsovereenkomst of andere geldende regeling voortvloeiende bevoegdheid of voorziening door de ondernemingsraad onaangetast.

15.3 ENGIE Energie Nederland N.V. en de ondernemingsraad van ENGIE Energie Nederland N.V. kunnen deze gedragscode in onderling overleg wijzigen of aanpassen. Deze wijzigingen worden schriftelijk vastgelegd en voorafgaand aan de invoering aan de medewerkers bekend gemaakt. Deze regeling wordt jaarlijks geëvalueerd door ENGIE en de centrale ondernemingsraad.