



# Tweede Kamer

DER STATEN-GENERAAL

## Gedragsregeling voor de digitale werkomgeving

### 1. Doelstelling gedragsregeling voor de digitale werkomgeving

Doel van de Gedragsregeling digitale werkomgeving is kamerambtenaren bekend te maken met de gedragsregels die leiden tot een verantwoord gebruik van de digitale werkomgeving. Tevens wordt duidelijk gemaakt op welke wijze controle op het gebruik ervan kan plaatsvinden.

Deze gedragsregeling komt in de plaats van de huidige Gedragscode internet- en e-mailgebruik (2014) en de huidige Gedragscode Sociale media (2011), die dus komen te vervallen en is een verbijzondering van de gedragscode integriteit.

De gedragsregeling geeft de marges aan, echter het is onmogelijk alle geboden en verboden limitatief op te sommen. In de gevallen waarin deze regeling niet voorziet komt het aan op het vermogen van de medewerker om zelfstandig op verantwoorde wijze te handelen. Iedere kamerambtenaar blijft zelf verantwoordelijk voor zijn of haar gedrag in zijn/haar digitale werkomgeving. Er wordt dan ook een beroep gedaan op het eigen morele besef en het gezonde verstand. De gedragscode Integriteit van de Tweede Kamer kan hierbij helpen.

### 2. Gedragsregeling voor de digitale werkomgeving

#### Artikel 1 Definities

In deze gedragsregeling wordt verstaan onder:

- a. Tweede Kamer: de ambtelijke organisatie van de Tweede Kamer der Staten-Generaal.
- b. Medewerker: de medewerker die werkzaamheden verricht voor de ambtelijke organisatie van de Tweede Kamer, ongeacht of hij in dienst is van de Tweede Kamer of is ingehuurd. Dus ook de stagiaire, de uitzendkracht en de ingeleende arbeidskracht.
- c. Digitale werkomgeving: bevat producten en diensten die aan een persoon worden toegekend en die plaats- en tijdonafhankelijk zijn, o.a. virtuele werkplek, toegangs-service (gebruikersnaam/wachtwoord), standaard applicaties, thuiswerkvoorziening (token) en mobiele apparaten zoals mobiele telefoon en tablet.
- d. Datalek: Hierbij gaat het om toegang tot of vernietiging, wijziging of vrijkomen van persoonsgegevens bij de Tweede Kamer, zonder dat dit de bedoeling is.
- e. MDM: Mobile Device Management is een verzamelnaam voor de apps die beheer van mobiele apparaten op afstand mogelijk maken. Het stelt de Tweede Kamer in staat Kamerdata beter te beveiligen. Na installatie van het MDM-oplossing "Citrix Secure Hub" is er niet alleen een betere beveiliging van de e-mail, maar kan de Tweede Kamer in het geval van verlies of diefstal de Kamerdata op het apparaat op afstand wissen.

## **Artikel 2 Digitale werkomgeving**

- a. De medewerker is zelf verantwoordelijk voor de handelingen die worden verricht onder de persoonlijke toegang (inloggegevens) tot de digitale werkomgeving.
- b. Ter beschikking gestelde apparatuur moet door de medewerker worden beveiligd met een pincode of een wachtwoord, conform het wachtwoordbeleid van de Tweede Kamer. Het is niet toegestaan inlognaam, wachtwoord of PUK-code van het apparaat aan derden bekend te maken.
- c. Verlies of diefstal van mobiele apparaten of gegevensdragers moet direct gemeld worden bij servicedesk 3060.
- d. De digitale werkomgeving mag naar redelijkheid en billijkheid ook voor persoonlijke doeleinden gebruikt worden. Wees ervan bewust dat berichten verstuurd vanaf een e-mailadres van de Tweede Kamer door de ontvanger worden gezien als een e-mail van de Tweede Kamer. Pas taalgebruik aan.
- e. Wees altijd zorgvuldig, betrouwbaar, integer en respectvol in je uitlatingen op sociale media<sup>1</sup>. Op internet kan iets snel teruggevonden worden en het blijft er ook altijd op staan. De Tweede Kamer respecteert de vrijheid van meningsuiting van haar werknemers. Maar wees ervan bewust dat persoonlijke meningen kunnen conflicteren met de belangen van de Tweede Kamer en dat het niet altijd verstandig is om de eigen mening online en openbaar te etaleren. Diensthoofden en leidinggevenden, en degenen die namens de Tweede Kamerorganisatie het beleid en de strategie uitdragen hebben een bijzondere verantwoordelijkheid bij het gebruikmaken van sociale media. Voor sommige functies geldt dat iemand altijd wordt verbonden aan de Tweede Kamer, ook als hij een privémening verkondigt. Bedenk dus tevoren welk effect een bijdrage op het internet (bericht, foto, video) heeft voor de Tweede Kamer. Bij twijfel wordt overlegd met de leidinggevende of stafdienst Communicatie.
- f. Een medewerker mag geen gebruik maken van de digitale werkomgeving om discriminerende, pornografische, beledigende of daarmee vergelijkbare uitingen te verzenden, bekijken of te ontvangen.

## **Artikel 3 Technische voorzieningen en procedures**

- a. De Tweede Kamer zorgt voor betrouwbare informatievoorzieningen. Dit wordt gewaarborgd door back-ups en technische beveiligingsmaatregelen. Inbreuk op beveiliging dient terstond gemeld te worden bij de servicedesk 3060.
- b. Binnen de Tweede Kamer zijn procedures van kracht omtrent het melden van datalekken. Een vermoeden van een datalek dient dit te worden gemeld aan de servicedesk 3060.
- c. De Nederlandse Rijksoverheid is doelwit van geavanceerde digitale aanvallen voor spionage, sabotage of zelfs terrorisme. Daarom heeft de Tweede Kamer technische voorzieningen ingericht die de betrouwbaarheid en weerbaarheid van de informatievoorziening van de Tweede Kamer waarborgen.

---

<sup>1</sup> Zie ook [artikel 50 lid 1 ARAR](#) over goed ambtenaarschap en [Gedragscode Integriteit pagina 5](#) over goed ambtenaarschap en de eigen verantwoordelijkheid.

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.

- d. Alleen de bij de Tweede Kamer bekende apparaten krijgen toegang tot de ICT-faciliteiten van de Kamer. Mobiele apparaten waarmee gebruikers toegang willen verkrijgen tot het Tweede Kamer-netwerk, bijvoorbeeld voor het raadplegen van hun email of agenda, dienen te zijn voorzien van MDM. Dat geldt voor alle mobiele apparaten, zowel privéapparaten als door de Tweede Kamer uitgegeven apparaten. Hiermee kan worden gewaarborgd dat in geval van verlies of diefstal het apparaat kan worden ontdaan van bedrijf kritische en/of privacygevoelige data.

#### **Artikel 4 Toezicht op naleving**

- a. De verantwoordelijkheid voor het toezicht op de naleving van deze Gedragsregeling ligt in eerste instantie bij de direct leidinggevende. De beveiligingsambtenaar (BVA) houdt namens de Griffier toezicht op de naleving. Niet naleving kan leiden tot maatregelen, zie artikel 6.
- b. Bij iedere overtreding van de gedragsregeling neemt de leidinggevende contact op met de BVA voor advies en overleg over vervolgacties, zoals melding aan het MT.

#### **Artikel 5 Controle op naleving**

- a. Om technische fouten en onregelmatigheden in een vroeg stadium te kunnen ontdekken en tijdig onderhoudsmaatregelen te kunnen treffen, wordt zowel het gebruik als de werking van de digitale werkomgeving geautomatiseerd vastgelegd (gelogd).
- b. Bij zwaarwegende feiten kan ook controle op de inhoud plaatsvinden, over een periode niet langer dan 6 maanden na de constatering van het zwaarwegende feit. Hierbij wordt gezorgd voor een juiste balans tussen enerzijds de controle en anderzijds de bescherming van de privacy van betrokkenen.
- c. In geval van onderzoek naar ernstige informatiebeveiligingsincidenten en de mogelijke gevolgen hiervan heeft de CISO of diens plaatsvervanger, na melding aan het MT, recht op toegang te krijgen tot alle dataverkeer.
- d. Bij langdurige afwezigheid moet in het kader van de continuïteit van de dienstverlening gezorgd worden dat een collega toegang heeft tot relevante informatie die zich bevindt in de digitale werkomgeving. In zeer bijzondere gevallen kan het diensthoofd of de leidinggevende bij de BVA of FG plaatsvervangende toestemming vragen.
- e. Bij specifieke functionarissen (zoals vertrouwenspersonen en leden van de OR) kunnen nadere regels worden gesteld voor de toegang tot het inlog-account en de digitale werkomgeving.

#### **Artikel 6 Sancties**

- a. Inbreuk op de Gedragsregeling voor de digitale werkomgeving wordt beschouwd als plichtsverzuim. Stafdienst HR heeft hier een coördinerende, controlerende en adviserende rol.

- b. Als misbruik wordt geconstateerd is de Tweede Kamer bevoegd tot het nemen van disciplinaire of arbeidsrechtelijke maatregelen tegen de medewerker(s), zoals schorsing, schriftelijke berisping of ontslag, als bedoeld in respectievelijk artikel 90 en 81, lid 1, onder a. en onder l. van het ARAR.
- c. In de afweging van de sanctie en acties bij een overtreding wordt betrokken:
- de ernst van de overtreding;
  - de directe (maatschappelijke) schade die de Tweede Kamer kan of heeft opgelopen;
  - de verstoring van de werkzaamheden en activiteiten van één of meerdere medewerkers van de Tweede Kamer;
  - de impact op de werkzaamheden van de overtreder.

Den Haag, 17 januari 2019



Simone Roos  
Griffier van de Tweede Kamer der Staten-Generaal