Handreiking informatieveiligheid en privacy voor raadsleden, commissieleden en bestuurders

Als raadslid, commissielid en bestuurder (burgmeester en wethouders) beschik je over ICT-middelen en informatie van de gemeente. Deze informatie is “de grondstof” voor je politieke en bestuurlijke werk. Wanneer deze informatie gelekt, gehackt of gemanipuleerd wordt kan dit aanzienlijke schade opleveren voor jouw positie en de gemeente Midden-Groningen.

Informatieveiligheid gaat over het nodig hebben (***B**eschikbaarheid*), kunnen vertrouwen (***I**ntegriteit*) en daar waar nodig geheimhouden (***V**ertrouwelijkheid*) van onze informatie.

Er zijn veel risico’s die de beschikbaarheid, integriteit en vertrouwelijkheid van de gemeentelijke informatie in gevaar kunnen brengen. Denk aan:

- Per ongeluk of expres lekken van informatie;
- Hacken, gijzelen of manipuleren van informatie;
- Techniek die niet meer goed werkt;
- Stroomstoringen en brand.

Via technische beveiliging, zoals het tegenhouden van virussen en hackers, beperken we 80% van de risico’s. Voor de overige 20% is jouw hulp en inzet nodig.

In deze handreiking geven we je richtlijnen mee om informatie- en privacy veilig je raads(commissie)- en bestuurlijke werk te doen.

Verschillende soorten gegevens

- ✓ **Openbare gegevens**: Alle gegevens die iedereen kan en mag zien;

- ✓ **Vertrouwelijke gegevens:** Dit zijn gegevens die alleen door bepaalde groepen personen te zien zijn. Denk hierbij aan (bijzondere) persoonsgegevens en personeelsgegevens. Bijvoorbeeld een curriculum vitae. Persoonsgegevens verdienen bijzondere aandacht. Dit zijn gegevens die over een persoon gaan en waardoor de persoon te herkennen is. Denk hierbij aan naam- en adresgegevens, e-mailadressen maar ook telefoonnummers van collega’s en inwoners. De gegevens worden gebruikt op basis van vertrouwen. Gebruik je deze gegevens onbedoeld/bedoeld niet juist, kan dit gevolgen hebben voor jou en de personen die betreft;

- ✓ **Geheime gegevens:** het gaat om zeer gevoelige gegevens die alleen gebruikt worden door één persoon of een beperkte groep personen. Als deze gegevens onbedoeld/bedoeld niet juist gebruikt worden, kan dit grote gevolgen hebben. Volgens de Gemeentewet en de Wet open overheid kan geheimhouding worden opgelegd.

Downloaden, bewaren en printen vertrouwelijke en geheime informatie

- ✓ Download geen geheime en vertrouwelijke informatie vanuit de informatiesystemen van de gemeente. Bewaar deze niet op privé apparaten en print ze niet. Gebruik deze informatie rechtstreeks vanuit het bronsysteem zoals het Raads- en bestuurlijk informatiesysteem, het zaaksysteem van de gemeente of de beveiligde vergader App.
- ✓ Dit geldt ook als je stopt met je werk als raads(commissie-)lid of bestuurder.

Gebruik ICT-middelen

- ✓ Je bent zelf verantwoordelijk voor de ICT-middelen die door de gemeente beschikbaar zijn gesteld. De apparaten leen je niet uit aan een ander. Laat iemand anders geen gebruik maken van de apparaten;
- ✓ Vergrendel je tablet, laptop of computer bij het verlaten van je plek.

Begeleiden van externe bezoekers in het Huis voor Cultuur en Bestuur

- ✓ Begeleid je externe bezoekers die geen toegang hebben tot de besloten delen van het gebouw. En laat ze er niet alleen achter.

Toegangsbeveiliging

Het beveiligen van toegang tot informatie begint met een goed wachtwoord, een authenticatie App en een goede pincode. Voor toegang tot de gemeentelijke informatiesystemen (zoals E-mail, Raads- en Bestuurlijke Informatiesysteem) en ICT-middelen worden de vereisten hiervan technisch afgedwongen.

- ✓ Het huidige wachtwoordbeleid is de toepassing van minimaal 13 tekens;
  - Een lang wachtwoord of een 'wachtzin' is beter dan een kort, complex wachtwoord;
  - Het wachtwoord moet 3 van de 4 onderstaande tekens hebben:
    - Hoofdletters (A tot en met Z)
    - Kleine letters (a tot en met z)
    - Cijfers (0 tot en met 9)
    - Speciale tekens (bijvoorbeeld !, $, # en %)
    - Het wachtwoord is 6 maanden geldig.

- ✓ Pincodes (op zakelijke telefoon of tablet) moeten minstens 6 tekens zijn. Geen 000000 of opvolgende nummerreeks (123456). Bij nieuwste mobiele telefoons en tablets kan ook gebruik gemaakt worden van gezichtsherkenning of vingerprint;

- ✓ Gebruik verschillende wachtwoorden voor privé- en professionele accounts;

- ✓ Gebruik verschillende wachtwoorden voor elke website en applicatie;

- ✓ Een digitale wachtwoordkluis kan je helpen

- ✓ Deel wachtwoorden en pincodes nooit, ook niet af en toe. Wachtwoorden en pincodes zijn persoonlijk.

Vergaderingen en gesprekken over raads- en bestuurlijk werk gerelateerde zaken

- ✓ Wees je ervan bewust dat je niet alles in bijzijn van collega's, partijgenoten, familieleden en vrienden kunt bespreken. Ook niet in het openbaar;

- ✓ Zorg bij online vergaderen of overleggen ervoor dat niemand mee kan luisteren. Tenzij het openbaar is.

Gebruik e-mail

- ✓ Gebruik het e-mailadres van de gemeente Midden-Groningen alléén voor raads- en bestuurlijk werk gerelateerde zaken. Werk informatie stuur je niet door naar privé e-mail;

- ✓ Voor het beveiligd verzenden van persoons- en vertrouwelijke gegevens naar mailadressen buiten de gemeentelijke organisatie kun je Zivver gebruiken. Deze is geïntegreerd in Outlook;

- ✓ Gebruik de zakelijke e-mail niet voor berichten met pornografische, racistische, discriminerende, beledigende, (seksueel) intimiderende of aanstootgevende inhoud of voor berichten die kunnen uitdagen tot haat en geweld;

- ✓ Bij mailberichten naar groepen buiten de gemeente Blind Carbon Copy (BCC) gebruiken;

- ✓ Voorkom phishing:
  - Controleer of de naam van de afzender klopt en wordt verwacht
  - Controleer of de link naar het verwachte webadres leidt door er met de muis overheen te gaan
  - Controleer of de naam en of een bijlage passend is voordat je deze opent of download

- ✓ Als je stopt als raads(commissie)lid of bestuurder mag je je zakelijke mailbox niet downloaden voor eigen gebruik als het gaat om vertrouwelijke en geheime informatie.

Je eigen mobiele device gebruiken voor toegang tot gemeentelijke informatie

- ✓ Wanneer je op je eigen mobiele device (Bring-Your-Own-Device/BYOD) gebruik wilt maken van bijvoorbeeld mail, Apps en data van de gemeente is dit mogelijk als die Apps en data op afstand beheerd worden door team Automatisering. Het beheer beperkt zich dan alleen tot die Apps en data van de gemeente (bijvoorbeeld Outlook App en RISBIS App). Bij verlies of vermissing van je device kan team Automatisering de gemeentelijke Apps en data op afstand wissen. Het gebruik van je eigen mobiele device zal verder niet worden beheerd of gevolgd door team Automatisering (geen toegang tot privé gegevens en Apps).

Internet en sociale media

- ✓ Denk na voordat je wat deelt via sociale media. Houd rekening met jouw positie als raadslid of bestuurder en de goede naam van de gemeente. Houd daarbij ook rekening met iedereen die erbij betrokken is;

- ✓ Deel via internet of sociale media geen vertrouwelijke en geheime informatie. Ook niet als je bijvoorbeeld gebruik maakt van kunstmatige intelligentie zoals ChatGPT. Je weet namelijk niet waar de ingevoerde informatie terecht, opgeslagen en weer gebruikt wordt;

- ✓ Gebruik geen dreigende, beledigende, seksueel getinte, racistische of discriminerende toon via online sociale netwerken en andere vergelijkbare communicatienetwerken. Dit geldt voor alle met de gemeente verbonden en betrokken activiteiten. Gebruik ook geen namen van ambtenaren;

- ✓ Maak bij onderwerpen die je openbaar maakt en met de gemeente te maken hebben duidelijk of je het namens jezelf of namens de gemeente doet;

- ✓ Maak beeldmateriaal niet openbaar van personen zonder toestemming van de persoon. Zorg dat je de toestemming schriftelijk aan kunt tonen als je het wel openbaar maakt;

- ✓ Weet dat openbaar maken van berichten op sociale media altijd vindbaar zijn en moeilijk te verwijderen;

- ✓ Je bent zelf verantwoordelijk voor wat je uitbrengt via internet en sociale media.

Melden van beveiligingsincidenten

Meld alle gebeurtenissen rond informatiebeveiliging en datalekken direct. Voor raadsleden kan dit via de griffie en bestuurders kunnen dit rechtstreeks melden in Topdesk of telefonisch via de ICT Servicedesk. Voorbeelden van beveiligingsincidenten zijn:

- ✓ Lekken van niet-openbare bedrijfsinformatie en persoonsgegevens. Bijvoorbeeld een mailbericht met persoonsgegevens dat aan verkeerde partij of organisatie is gestuurd;
- ✓ Stelen of vermissing toegangspas of sleutels;
- ✓ Stelen of misbruik van je gebruikersnaam en wachtwoord;
- ✓ Stelen of vermissing van ICT-bedrijfsmiddelen (telefoon, tablet, chromebook, laptop);
- ✓ Phishing: Een internetcrimineel probeert via een mailbericht of criminele website geld of inloggegevens te stelen.

Deze richtlijnen gelden overal: op kantoor, thuis, in de trein, waar dan ook. Kortom: wees je bewust van de risico's. Let op je ICT-middelen, informatie én op je woorden.

En help elkaar in de bewustwording van risico's op het gebied van informatieveiligheid & privacy door het gesprek erover te voeren of eigen voorbeelden waar het mis bespreekbaar te maken.