



Richtlijnen veilig doorsturen van gevoelige gegevens via O365

Medewerkers moeten extra maatregelen nemen bij het versturen van gevoelige documenten via Outlook of andere O365 tools van Microsoft om zodoende te voorkomen dat vertrouwelijke informatie in verkeerde handen valt. Deze maatregelen helpen ook om te voldoen aan wet- en regelgeving, zoals de GDPR, en beschermen de belangen van het bestuur door de integriteit en vertrouwelijkheid van gegevens te waarborgen. Door zorgvuldig om te gaan met gevoelige informatie kunnen besturen reputatieschade en juridische problemen voorkomen.

Gevoelige gegevens omvatten een breed scala aan informatie die essentieel is voor zowel individuen als het bestuur en extra bescherming vereist. Dit omvat alle persoonsgegevens, en met name de bijzondere categorieën van persoonsgegevens zoals raciale afkomst, politieke overtuigingen, gezondheidsinformatie en seksuele geaardheid. Daarnaast betreft het ook bedrijfskritische informatie zoals financiële gegevens, intellectuele eigendommen, bedrijfsstrategieën, juridische documenten en cruciale operationele en netwerkgegevens.

Het is dan ook belangrijk dat je voorzorgen neemt bij het versturen van gevoelige gegevens om de integriteit en de vertrouwelijkheid van deze gegevens te waarborgen en ze te beschermen tegen ongeautoriseerde toegang en lekken. Hieronder geven we 8 eenvoudige maatregelen die je hierbij moet hanteren.

1. Dubbelcheck als de gegevens mogen worden doorgegeven

Burgers, bedrijven, organisaties, andere overheden... vragen dagelijks gevoelige gegevens op bij het lokaal bestuur. De vraag alleen betekent natuurlijk niet dat we deze gegevens zomaar mogen doorgeven. We moeten ons als bestuur aan de GDPR en andere wetgeving houden en daarnaast kan het schadelijke gevolgen hebben als we bedrijfskritische gegevens met verkeerde mensen delen. Bij twijfel kan je raad vragen aan je diensthoofd of de data protection officer.

2. Dubbelcheck het adres van de geadresseerden

Vaak vult Outlook automatisch e-mailadressen aan. Hier schuilt het risico in dat je gegevens per ongeluk verzendt naar een onbevoegde geadresseerde die dezelfde voor- of achternaam heeft als de bedoelde bestemming.

Dubbelcheck daarom steeds het adres van je bestemming vooraleer je op 'Verzenden' klikt.

3. Versleutel de e-mail

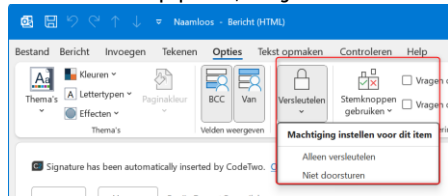
Bij het opmaken van de e-mail, ga je naar het menu 'Opties' en kiest daar voor 'Versleutelen'.

De ontvanger krijgt een bericht dat hem een versleutelde e-mail werd toegestuurd.

Alleen de beoogde ontvanger, die de juiste sleutel of certificaat heeft om de e-



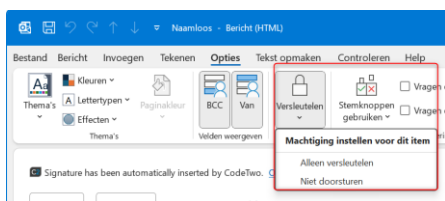
mail te ontsleutelen, kan de inhoud lezen. Voor anderen die de e-mail proberen te onderscheppen, blijft de inhoud onleesbaar.



4. Zorg dat geadresseerden je e-mail niet kunnen doorsturen

Bij het opmaken van de e-mail, ga je naar het menu 'Opties' en kiest daar voor 'Versleutelen' en 'Niet doorsturen'.

Het selecteren van deze optie zorgt ervoor dat de geadresseerde het bericht de bijlages kan lezen, maar het bericht niet doorsturen, afdrukken of de inhoud ervan kopiëren.



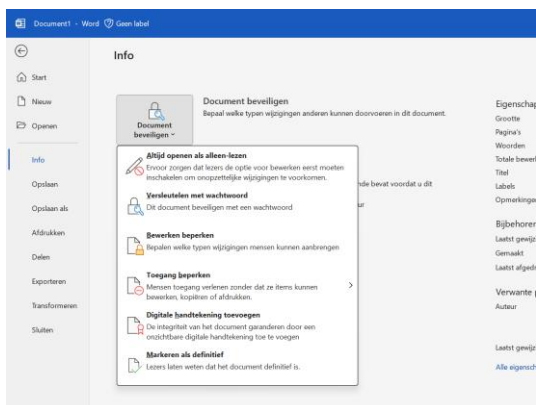
5. Versleutel de e-mailbijlage

De courante Office-pakketten bieden je de mogelijkheid om bestanden te versleutelen (of te encrypteren).

Als je bij een Office-bestand op 'Bestand' en vervolgens 'Info' klikt, krijg je de optie 'Document beveiligen' te zien.

Daar kan je kiezen voor 'Versleutelen met wachtwoord'.

Bezorg het wachtwoord echter altijd via een ander medium aan de geadresseerde (via de telefoon, een SMS of WhatsApp-bericht).



6. Stel het versturen van je e-mail uit

Stel je kort na het verzenden vast dat je een niet-versleuteld bericht toch nog naar een verkeerde bestemming hebt verstuurd, breng de ontvanger op de hoogte van dit feit en vraag om het bericht in kwestie onmiddellijk te verwijderen.

Maak er echter een gewoonte van om berichten uitgesteld te versturen. Door een bezorgdatum en -tijd in te stellen, kun je je e-mails controleren en eventuele fouten corrigeren voordat ze daadwerkelijk worden verzonden. Na het klikken op



'Verzenden', wordt de e-mail opgeslagen in je 'Postvak UIT', waar je hem kunt herzien en aanpassen tot het moment van verzending.

Hoe stel je een dergelijke regel in?

Start door je e-mail op te stellen in Outlook en navigeer naar het tabblad 'Opties'.

Kies vervolgens 'Bezorging uitstellen'. In het dialoogvenster 'Eigenschappen' selecteer je 'Niet bezorgen voor' om de gewenste datum en tijd in te stellen.

7. Deel documenten via SharePoint, Teams of OneDrive

Documenten kunnen, behalve via e-mail, ook via SharePoint, Teams of OneDrive gedeeld worden.

Gebruik enkel specifieke e-mailadressen en vermijd het gebruik van 'Iedereen met de link'-opties. Indien mogelijk, stel documentinstellingen in zodat externen alleen leesrechten hebben. Stel ook telkens een vervaldatum in zodat documenten maar tijdens een beperkte periode gedeeld worden.

Hoe een document correct delen via SharePoint, Teams of OneDrive?

1. Selecteer het document dat je wilt delen.
2. Klik op de knop 'Delen'.
3. Kies 'Specifieke personen' in plaats van 'Iedereen met de link'.
4. Voer de e-mailadressen van de ontvangers in.
5. Zet de toestemmingen op 'Alleen weergeven', tenzij de ontvanger moet kunnen bewerken.
6. Stel een vervaldatum in voor de toegang.
7. Klik op 'Verzenden' en bevestig dat je alle stappen correct hebt gevolgd.

8. Gebruik geen andere systemen voor de doorgifte van documenten

In het kader van de beveiliging van gevoelige gegevens binnen onze organisatie, is het uitsluitend toegestaan om gevoelige informatie te delen via de bovenstaande werkwijzen. Zo garanderen we dat gevoelige informatie alleen door geautoriseerde ontvangers kan worden ingezien.

Het gebruik van andere methoden (zoals WeTransfer, Dropbox, WeSendit, Google Cloud of vergelijkbare platforms) voor het delen van gevoelige gegevens is niet toegestaan. Deze platforms bieden onvoldoende garanties op het gebied van veiligheid en kunnen leiden tot ongewenste risico's voor de integriteit en vertrouwelijkheid van de data.

Het gebruik van USB-sticks, externe harde schijven en andere draagbare opslagmedia voor het opslaan of delen van gevoelige gegevens wordt sterk afgeraden. Dergelijke apparaten vormen een aanzienlijk beveiligingsrisico, omdat ze gemakkelijk verloren kunnen gaan, gestolen kunnen worden of ongewenst kunnen worden gebruikt door onbevoegden. Het is moeilijk om de juiste encryptie en beveiligingsmaatregelen te waarborgen op deze draagbare media. Wij raden daarom aan om altijd gebruik te maken van hierboven beschreven werkwijzen voor het delen van gevoelige informatie.

Het niet naleven van deze richtlijnen kan ernstige gevolgen hebben en wordt beschouwd als een schending van ons informatiebeveiligingsbeleid.



Wij rekenen op ieders medewerking om de veiligheid van het bestuur en onze burgers te waarborgen.

Hulp nodig?

Neem contact op met dienst ICT.