10 Gouden regels voor cyberveiligheid

Sjabloon

# Autoriteit en herziening

## Documentcontrole en beoordeling

|  |  |
| --- | --- |
| **Documentcontrole** |  |
| Auteur |  |
| Eigenaar |  |
| Datum aangemaakt |  |
| Laatst herzien door |  |
| Laatste herzieningsdatum |  |

.

## Versiebeheer

|  |  |  |  |
| --- | --- | --- | --- |
| **Versie** | **Datum van goedkeuring** | **Goedgekeurd door** | **Beschrijving van verandering** |
| 1.0 |  |  |  |

# 10 Gouden regels voor cyberveiligheid

|  |  |
| --- | --- |
|  | **Bescherm je accounts met sterke authenticatie!**  **Gebruik steeds waar mogelijk multifactor-authenticatie (MFA)!**   * Lange wachtwoorden zijn efficiënter omdat ze voor cybercriminelen moeilijker te kraken zijn, gezien de vele mogelijkheden die het aantal tekens biedt. * Sterke wachtwoorden zijn **minstens 14 tekens lang, zijn niet gemakkelijk te achterhalen en bevatten: hoofdletters, kleine letters, numerieke tekens, speciale tekens (&,$,%,!,=,+..).** |
|  | Gebruik verschillende wachtwoorden voor professionele en persoonlijke accounts |
|  | Sla al je gegevens op in een systeem waar regelmatig en centraal back-ups worden gemaakt. |
|  | Voer beveiligingsupdates uit op al je apparaten zodra deze beschikbaar zijn |
|  | Laat nooit fysieke informatie (bijv. papieren) of apparaten onbeheerd achter op je bureau |
|  | Vermijd openbare Wi-Fi en gebruik het Virtual Private Network (VPN) van de organisatie |
|  | **Vermijd phishing door jezelf de volgende vragen te stellen**:   * Is de verzender iemand die ik ken? * Verwachtte ik een bericht over het vermelde onderwerp? * Vraagt het bericht om informatie zoals een gebruikersnaam, een paswoord of een bankrekeningnummer? * Is het dringend? * Waarheen leidt de link? (ga er alleen met je muis over, niet klikken) * Bevat het bericht een QR-code? * Word ik persoonlijk aangesproken? * Staan er taalfouten in het bericht? * Zit het bericht in de map Spam / Junkmail? * Probeert iemand mij nieuwsgierig te maken? * Wordt er om een betaling gevraagd?   **Hoe reageer je op een phishing-e-mail?**   * Antwoord er niet op, open geen enkele bijlage en klik niet op de links. * Deel nooit bankgegevens waar via sms of e-mail om wordt gevraagd. * Meld de poging tot phishing aan **[IT-afdeling/provider]** en verwijder de e-mail/tekst. |
|  | Neem de volgende maatregelen in acht bij de behandeling van interne of vertrouwelijke informatie:   * Vergrendel je computer als je hem onbeheerd achterlaat. * Laat geen computers of papieren onbeheerd achter op bureaus buiten de werkuren. * Laat geen papieren onbeheerd achter in printers. * Let altijd op je omgeving wanneer je vertrouwelijke informatie raadpleegt of bespreekt in openbare ruimtes. Probeer je waar mogelijk af te zonderen om te voorkomen dat iemand een gesprek afluistert |
|  | Gebruik alleen officiële websites en platforms om applicaties en software te downloaden. Het downloaden van software moet vermeden worden. Software wordt geïnstalleerd door **de IT-afdeling/provider.** |
| Marketing outline | Meld alle informatiebeveiligingsincidenten aan je IT-afdeling/provider Neem altijd contact op met **[IT-afdeling/provider]** wanneer:  je vragen of opmerkingen hebt over dit document;   * je iets opmerkt dat in strijd is met dit document; * er zich een vermoedelijk of bevestigd incident voordoet.   Contactgegevens: **[IT-afdeling/provider telefoonnummer] / [IT-afdeling/provider e-mail]** |