

WELKOM

IT-security is teamwork

- Digitale veiligheid begint bij ons allemaal.
- Stop bij twijfel, controleer en meld.



01

HERKENNEN

Herken phishing en social engineering

- Wees alert voor onverwachte links, bijlagen, QR-codes en dringende verzoeken.
- Phishing komt ook via Teams, sms, QR-codes en telefoon.



02

REAGEREN

Meld verdachte situaties onmiddellijk

- Verdachte mail, vreemde MFA-melding, fout bestand geopend of iets gewijzigd?
- Meld het meteen — ook als je al hebt geklikt.



03

CONTROLLEREN

Controleer gevoelige verzoeken

- Een vraag om geld, wachtwoorden, bestanden of gewijzigde bankgegevens?
- Controleer die altijd via een tweede, vertrouwd kanaal.



04

AANMELDEN

Gebruik MFA veilig

- Gebruik MFA voor iedere toepassing die dit aanbiedt.
- Keur nooit een aanmelding goed die je niet zelf hebt gestart.



05

AANMELDEN

Bescherm je wachtwoorden

- Gebruik voor elke account een uniek wachtwoord en deel het nooit.
- Bewaar wachtwoorden nooit op post-its of in onbeveiligde bestanden.



06

INFORMATIE

Behandel bedrijfsinformatie als vertrouwelijk

- Productiefoto's, prijslijsten, klantenlijsten, offertes en planningen zijn vertrouwelijk.
- Deel ze alleen met bevoegden via goedgekeurde kanalen.



07

INFORMATIE

Gebruik alleen goedgekeurde opslag

- Bewaar bedrijfsinformatie uitsluitend in de goedgekeurde bedrijfsomgeving.
- Nooit op privétoestellen of persoonlijke Google Drive-, Dropbox- of cloudaccounts.



08

INFORMATIE

Gebruik AI op een veilige manier

- Geen klantdata, contracten, cijfers, wachtwoorden of broncode in publieke AI-tools.
- Gebruik uitsluitend AI-toepassingen die door het bedrijf zijn goedgekeurd.



09

TOESTELLEN

Automatische updates op je toestel

- Updates worden automatisch geïnstalleerd.
- Werkt een update niet? Meld het aan IT.



TOESTELLEN

Installeer niets op eigen initiatief

- Installeer geen software, browserextensies of gratis PDF-tools zonder toestemming.
- Vraag bij twijfel eerst advies aan IT.



11

TOESTELLEN

Wees voorzichtig met USB en hardware

- Sluit USB-sticks, externe schijven, laders of gadgets alleen aan na toestemming.
- Een gevonden USB-stick sluit je nooit aan.



12

MOBIEL

Beveilig je smartphone

- Houd automatische updates aan en installeer apps alleen via officiële stores.
- Beveilig je toestel met een pincode of biometrische vergrendeling.

**13**

MOBIEL

Werk veilig onderweg

- Vermijd onbekende openbare wifi; gebruik mobiele data of een vertrouwd netwerk.
- Verlies of diefstal van een toestel meld je onmiddellijk.



14

FYSIEK

Bescherm toestellen en werkplek

- Laat laptop of smartphone nooit zichtbaar of onbeheerd achter, ook niet in de wagen.
- Neem ze mee of berg ze veilig op en uit het zicht.



15

FYSIEK

Bewaak de fysieke toegang

- Laat onbekenden niet meelopen door beveiligde deuren en
leen je badge nooit uit.
- Laat vertrouwelijke documenten niet onbeheerd achter.

**16**

SAMEN

Twijfel? Meld het

- Geen schrik en geen schuld: snel melden helpt ons de schade beperken.
- Liever tien keer te veel gemeld dan één keer te weinig.

geert@altoni-kelderman.be



17