

# THUISWERKEN BIJ DE TU DELFT

## Waar moet ik op letten?

- Gebruik waar mogelijk je laptop of systeem van de TU Delft
- Gebruik Citrix alleen wanneer noodzakelijk
- Gebruik VPN alleen wanneer noodzakelijk
- Werk veilig

Je laptop van de TU Delft is ingericht om veilig te werken met de programma's die je nodig hebt. Gebruik deze dus waar mogelijk.

De TU Delft heeft een beperkt aantal licenties voor Citrix. Gebruik daarom Citrix alleen als er geen andere mogelijkheid is. **Vergeet niet om na gebruik direct uit te loggen uit Citrix.**

De TU Delft heeft beperkte capaciteit voor VPN. Gebruik daarom VPN alleen als er geen andere mogelijkheid is.

Verderop in dit document vind je **aanwijzingen en instructies over veilig werken**. We verzoeken je deze nauwkeurig op te volgen.

## Hoe kan ik sommige veelgebruikte programma's thuis gebruiken zonder Citrix?

### Applicatie

### Op een TU Delft laptop/systeem

### Op een privécomputer

#### E-mail

Gebruik Outlook of het mailprogramma dat je normaal ook gebruikt voor je werk. Via [webmail.tudelft.nl](http://webmail.tudelft.nl) kun je ook bij je e-mail; log in met je NetID en wachtwoord.

Ga naar [webmail.tudelft.nl](http://webmail.tudelft.nl). Je kunt inloggen met je NetID en wachtwoord.

#### Microsoft Office

De Microsoft Office suite (Word, Excel, Powerpoint) staat al geïnstalleerd op je laptop/systeem.

Installeer de Microsoft Office suite (Word, Excel, Powerpoint) als je deze nog niet hebt. De installatiehandleiding vind je [hier](#).

#### Bestanden (H:\, M:\ en andere netwerk-schijven)

Gebruik Webdrive. Hoe dat werkt, vind je [hier](#).

Gebruik Webdrive, maar zorg er voor dat je privécomputer voldoet aan de vereisten voor veilig werken (zie verderop). De handleiding voor het downloaden van Webdrive vind je [hier](#).

#### Sharepoint

Via <http://teams.connect.tudelft.nl/> kun je Sharepoint in elke webbrowser bereiken. Log in met je NetID en wachtwoord. Meer informatie vind je [hier](#).

#### Bellen, chat & online vergaderen (audio & video)

Skype voor Business staat ook al geïnstalleerd op je systeem. De andere partij hoeft niet te beschikken over Skype, maar kan een vaste of mobiele telefoon gebruiken. Lees de handleiding [hier](#).

Installeer Skype voor Business. De installatiehandleiding vind je [hier](#). De andere partij hoeft niet te beschikken over Skype for Business, maar kan een vaste of mobiele telefoon gebruiken.

## Bij het inloggen in een applicatie wordt mij gevraagd een *access code* in te voeren, klopt dat?

Ja, deze applicaties vragen om een *access code*:

- Basware Alusta
- Collegerama
- TIM
- Topdesk
- Tableau

Bij verschillende applicaties gaat het inloggen vanuit huis anders dan vanaf de campus. Deze applicaties maken gebruik van een dubbele beveiliging. Hierbij heb je naast je NetID en wachtwoord ook een code nodig om in te kunnen loggen. Deze code ontvang je per sms op het telefoonnummer dat de TU Delft van jou geregistreerd heeft.

### Ik weet niet of mijn mobiele nummer is geregistreerd.

Je kunt dit nakijken via: <https://e-service.tudelft.nl>.

### Mijn mobiele nummer is niet geregistreerd.

Neem telefonisch contact op met je [servicepunt](#); na controle van je gegevens wordt je mobiele nummer geregistreerd.

### Mijn mobiele nummer is niet juist geregistreerd.

Neem telefonisch contact op met je [servicepunt](#), na controle van je gegevens wordt je mobiele nummer geregistreerd.

## Ik heb via mijn webbrowser geen toegang tot de applicatie die ik wil gebruiken.

Verschiede applicaties van de TU Delft zijn vanuit huis niet benaderbaar via een webbrowser. Deze applicaties zijn alleen te gebruiken via Citrix.

Om Citrix te gebruiken (en eventueel te installeren) kan je gebruik maken van de handleiding via deze [link](#).

**Probeer het gebruik van Citrix te beperken en log iedere keer na gebruik uit op de volgende manier: meld je af via Startmenu en *Disconnect* en log uit door op je naam te klikken en te kiezen voor *Log off*. Op deze manier komt de Citrixlicentie direct weer beschikbaar voor een collega.**

Met de browserextensie Library Access heb je snel en eenvoudig toegang tot digitale inhoud zoals artikelen en tijdschriften, waar en wanneer je maar wilt. Voor de extensie, een handleiding en meer informatie, kijk [hier](#).

## Ik moet mijn NetID-wachtwoord wijzigen. Hoe doe ik dat vanuit huis?

### Met een laptop of systeem van de TU Delft:

Ga naar: <https://password.tudelft.nl/>. Log in met je NetID en je huidige wachtwoord. Je kunt nu je wachtwoord wijzigen. De wijziging is meteen van kracht. Outlook zal bijv. meteen om je nieuwe wachtwoord vragen.

NB: Bij het opstarten van je laptop en opnieuw aanmelden bij Windows blijft je oude wachtwoord voorlopig van kracht. **Je hebt dus tijdelijk twee wachtwoorden.** Zodra je weer op de campus bent en je laptop opnieuw opstart, is dit verholpen. Dit heeft verder geen gevolgen of beperkingen in het gebruik van de laptop of applicaties.

### Met een privécomputer:

Ga naar: <https://password.tudelft.nl/>. Log in met je NetID en je huidige wachtwoord. Je kunt nu je wachtwoord wijzigen. De wijziging is meteen van kracht.

## Hoe kan ik zorgen dat ik vanuit huis veilig kan werken?

Maak alleen gebruik van vertrouwde en beveiligde WiFi.

Gebruik waar mogelijk altijd je laptop of systeem van de TU Delft

Mocht je genoodzaakt zijn een privécomputer te gebruiken, zorg dan dat je de volgende maatregelen hebt getroffen:

- Gebruik geen verouderde versie van het besturingssysteem
- Stel een wachtwoord in voor toegang tot je privécomputer
- Zorg dat je een firewall en antivirusprogramma hebt geïnstalleerd en dat deze automatisch updates ontvangen
- Zorg dat updates van je besturingssysteem automatisch worden geïnstalleerd
- Gebruik software zoals aangeboden door TU Delft via [software.tudelft.nl](https://software.tudelft.nl)
- Versleutel je privécomputer

### Hoe beveilig ik mijn (WiFi)netwerk?

De minimaal benodigde maatregelen vind je via deze [link](#) en deze [link](#).

### Hoe krijg ik het meest recent besturingssysteem op mijn privé computer?

*Windows:* De overstap naar Windows 10 is nog steeds gratis (mits je een legitieme oudere versie van Windows hebt). Meer informatie vind je [hier](#).

*macOS:* Apple ondersteunt een behoorlijk aantal oudere versies van macOS met een actief updatebeleid. Meer informatie over het overstappen naar een recentere versie van macOS vind je [hier](#).

### Hoe kan ik een wachtwoord instellen op mijn privécomputer?

*Windows:* Informatie over het instellen van een wachtwoord voor Windows vind je [hier](#).

*macOS:* In macOS staat standaard een wachtwoord ingesteld. Je hoeft daar verder geen handeling voor uit te voeren.

### Hoe beveilig ik mijn privécomputer met een firewall en antivirussoftware?

*Windows:* Gebruik de in Windows 10 ingebouwde firewall en antivirussoftware van Microsoft. Meer informatie over het gebruik van de ingebouwde firewall, antivirusprogramma en andere maatregelen vind je [hier](#).

*macOS:* Voor het instellen van de firewall voor macOS, kijk [hier](#). Voor overige beveiligingsmaatregelen voor Mac, kijk [hier](#). (Informatie in het Engels).

### Hoe zorg ik dat updates automatisch worden geïnstalleerd op mijn privécomputer?

*Windows:* Updates in Windows 10 staan standaard aan. Schakel deze niet uit. Tips om updates te plannen en andere tips vind je [hier](#). Voor het gelijktijdig updaten van andere Microsoft programma's (Office), kijk [hier](#).

*macOS:* Updates van macOS en andere programma's kunnen eenvoudig uitgevoerd worden. Meer informatie vind je [hier](#).

### Hoe kan ik mijn privécomputer versleutelen?

Een handleiding voor het versleutelen van je privécomputer vind je [hier](#) (alle besturingssystemen).

## Ga zorgvuldig om met gegevens van de TU Delft en jezelf en houd deze veilig

- Zet geen gegevens van de TU Delft op je privécomputer, externe disk, USB-stick of andere fysieke drager
- Maak gebruik van [webdata.tudelft.nl](http://webdata.tudelft.nl), Webdrive of SURFdrive voor het opslaan of delen van gegevens
- Houd zakelijk gebruik gescheiden van privégebruik, stuur bijvoorbeeld geen zakelijke e-mail via je privémail
- Zorg dat gegevens niet toegankelijk zijn voor onbevoegden: lock ook thuis je scherm en zorg dat papieren documenten opgeborgen zijn in een afsluitbare lade, kast of ruimte
- Zorg dat je laptop of privécomputer geen aantrekkelijk doelwit is voor dieven of andere criminelen

### Wees alert op phishing en CEO-fraude

Helaas zien wij ook in deze omstandigheden een toename in het aantal e-mails met phishing en CEO-fraude

Ga niet in op verzoeken tot betalingen of aanschaf van giftcards, die lijken af te komen van je leidinggevende. Gebruik in geval van betalingen of verzoeken altijd de interne TU Delft-processen

Meld phishing, CEO-fraude of ander misbruik van TU Delft ICT via: [abuse@tudelft.nl](mailto:abuse@tudelft.nl)

## Veelgestelde vragen

### Ik heb thuis geen internet, wat nu?

Je kunt een *hotspot* maken met je mobiele telefoon. Zie hiervoor de handleidingen bij de provider van je telefoonabonnement.

### Hoe kan ik thuis gebruik maken van een TU Delft-werkplek?

Neem contact op met je leidinggevende om te kijken wat de mogelijkheden zijn, ook als je thuis een (extra) beeldscherm, een docking station, toetsenbord of muis nodig hebt. Neem alleen onderdelen mee van je eigen normale werkplek. **Het is nadrukkelijk niet de bedoeling om desktops mee naar huis te nemen.**

### Hulp nodig?

### Vraag of probleem melden?

Maak een melding via het self-service-portaal via deze [link](#). Log in met NetID en wachtwoord en kies vervolgens voor *Report to service desk*.