Kennisveilige internationale reizen

Protocol voor kennisveiligheid, informatiebeveiliging en bescherming van persoonsgegevens tijdens internationale reizen met dienstapparatuur ter informatie en instructie

Samengesteld door betrokkenen van Adviesgroep Kennisveiligheid, Integrale Veiligheid en de Chief Information Security Officer.

Inhoudsopgave

1. Inleiding 3
2. Uitgangspunten en beleidsprincipes 4
3. Risicobeoordeling kennisveiligheid bij reizen met dienstapparatuur 5
   Aanvullende risico inschatting 7
4. Voorbereiding op elke dienstreis 8
   A. Privéreizen en privé apparatuur tijdens reizen met dienstapparatuur 8
   B. Voorbereiding bij een dienstreis naar een land met een **Groen** risicoprofiel 9
   C. Voorbereiding bij een dienstreis naar een land met een **Geel** of **Oranje** risicoprofiel . 9
   D. Voorbereiding bij een dienstreis naar een land met een **Rood** risicoprofiel 10
5. Tijdens de dienstreis 11
   A. Dienstreis naar een land met een **Groen** risicoprofiel 11
   B. Dienstreis in een land met een **Geel** of **Oranje** risicoprofiel 12
   C. Dienstreis in een land met een met een **Rood** risicoprofiel 13
6. Na afloop van de dienstreis 14
7. Belangrijke Contacten 14

Bijlage 1. Uitleg en gebruik Reislaptop 16

Bijlage 2. Bestellen en installeren van de eSIM 19

1. Inleiding

Interne en externe medewerkers (zie 2c) van de Vrije Universiteit Amsterdam (hierna: VU) reizen regelmatig naar het buitenland om conferenties bij te wonen, onderwijs of trainingen te verzorgen, internationale samenwerkingen op te zetten en/of onderzoek uit te voeren. Deze reizen bieden waardevolle kansen om netwerken uit te breiden en kennis te delen. Tegelijkertijd brengen zakelijke reizen risico's met zich mee op het gebied van kennisveiligheid, informatiebeveiliging en de bescherming van persoonsgegevens. Zeker wanneer de reis naar een land gaat met een hoger kennisveiligheidsrisico. In dergelijke landen zijn er extra dreigingen, zoals het verplicht afgeven van mobiele apparatuur en inloggegevens bij inreizen, overheidsmonitoring en afluisterpraktijken. Buitenlandse statelijke actoren en andere belanghebbenden hebben mogelijk interesse in jou en de kennis die je bij je draagt. Daarnaast wordt de persoonlijke levenssfeer van individuen in sommige landen niet op dezelfde manier gerespecteerd als in Nederland.

Om de risico's op (digitale) spionage, onbedoelde kennisoverdracht of heimelijke beïnvloeding te verkleinen, moeten er bij reizen naar risicolanden voorzorgsmaatregelen genomen worden. Dit protocol voor reizen met dienstapparatuur richt zich specifiek op kennisveiligheid, als aanvulling op het algemene reis- en informatiebeveiligingsbeleid van de VU. In dit protocol wordt er onderscheid gemaakt tussen landen met verschillende risicoprofielen voor kennisveiligheid; hoe hoger het risicoprofiel van het land hoe zwaarder de aanvullende maatregelen.

Het protocol biedt medewerkers richtlijnen voor kennis- en informatieveilige reizen. Ook worden er aanbevelingen gedaan over gedrag op basis van de richtlijn "Op reis naar het buitenland" van de AIVD. In het geval van reizen naar landen met een (hoog) risicoprofiel schrijft het protocol het gebruik van speciale reisapparaten voor, om risico's op toegang tot gevoelige informatie te reduceren. Dit protocol biedt hiermee een kader voor het (beoordelings)proces voor het nemen van extra maatregelen tijdens reizen met dienstapparatuur en voor het aanvragen van de reisapparatuur (reislaptop en reistelefoon). Hiermee draagt het protocol bij aan het doel om kennisveiligheid niet alleen binnen, maar ook buiten de VU te borgen.

2. Uitgangspunten en beleidsprincipes

Voor dit protocol gelden de volgende beleidsprincipes:

a. Dit reisprotocol kennisveiligheid is aanvullend op, en vloeit voort uit diverse beleidskaders: het VU Kader Kennisveiligheid beschikbaar op de intranetpagina van kennisveiligheid[1], het VU-reisbeleid beschikbaar op de intranetpagina van Internationale Mobiliteit[2] en het VU-informatiebeveiligings[3]- en privacybeleid[4].
b. De doelgroep voor deze maatregelen zijn alle medewerkers van de VU die reizen maken met dienstapparatuur buiten Nederland. Onder medewerkers wordt verstaan alle in- en externe medewerkers, die werkzaamheden voor de VU verrichten, zoals student-assistenten, ingehuurde externe medewerkers en medezeggenschapsleden. Studenten vallen op dit moment buiten deze regeling.
c. Het is de verantwoordelijkheid van iedere medewerker om vóór vertrek de kennisveiligheidsrisico's van een dienstreis in te schatten door het reisadvies en het risicoprofiel van het bestemmings- en doorreislanden te beoordelen. Het doel hiervan is om eventuele risico's te verkleinen tot een acceptabel niveau, waarbij maatregelen proportioneel worden ingezet. Wanneer er sprake is van een verhoogd risico voor kennisveiligheid, wordt de contactpersoon kennisveiligheid van de eigen eenheid ingeschakeld. Deze adviseert de medewerker en de directeur bedrijfsvoering over de risicobeoordeling en de benodigde vervolgstappen om tot een onderbouwd advies te komen.
d. De directeur bedrijfsvoering van de faculteit of dienst is eindverantwoordelijk voor de uitvoering van kennis- en informatieveiligheid bij reizen met dienstapparatuur. Medewerkers voeren het beleid uit in samenwerking met IT, waarbij de IT-servicedesk zorgdraagt voor het beschikbaar stellen van reislaptops en mobiele telefoons. De CISO en de adviesgroep kennisveiligheid stellen de kaders vast en adviseren zowel de contactpersonen kennisveiligheid als de centrale informatiebeveiligers van de eenheden, en leveren daarnaast specifiek advies over informatiebeveiliging bij reizen met dienstappratuur.

[1] https://vu.nl/nl/medewerker/onderwijs-en-onderzoeksbeleid/kennisveiligheid-voor-vu-medewerkers

[2] https://vu.nl/nl/medewerker/internationalisering/internationaal-reisbeleid-voor-medewerkers

[3] https://vu.nl/nl/medewerker/informatiebeveiliging/Beleidsbibliotheek

[4] https://vu.nl/nl/medewerker/mijn-gegevens/persoonsgegevens-van-medewerkers-verwerken

3. Risicobeoordeling kennisveiligheid bij reizen met dienstapparatuur

Bij het plannen van een reis is het allereerst belangrijk om te beoordelen of het land of de regio van bestemming een verhoogd risicoprofiel voor kennisveiligheid heeft. Deze beoordeling staat los van, en kan verschillen van, de kleurcodes die het ministerie van Buitenlandse Zaken hanteert in het algemene VU-reisbeleid. De kennisveiligheidsbeoordeling vormt daarmee een **aanvullende stap** op de bestaande reisadviezen van Buitenlandse Zaken[5].

De VU baseert de risicobeoordeling voor kennisveiligheid tijdens internationale reizen met dienstapparatuur op het beleid uit de Nationale Leidraad Kennisveiligheid [6] , het VU-Kader Kennisveiligheid[7] en de openbaar beschikbare dreigingsinformatie van de inlichtingendiensten. De risico inschatting wordt vastgesteld door de Adviesgroep Kennisveiligheid en de CISO én wordt minimaal jaarlijks geactualiseerd. Voor deze actualisatie wordt gebruikgemaakt van onder meer de volgende dreigingsinformatie:

1. Het Dreigingsbeeld Statelijke Actoren 2025[8] van het Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV) en de meest recente jaarverslagen van de Algemene Inlichtingen- en Veiligheidsdienst (AIVD) en de Militaire Inlichtingen- en Veiligheidsdienst (MIVD). Hier wordt beschreven welke landen offensieve cyberprogramma's hebben die ingezet worden voor spionage. De landen die hierover beschikken, worden in dit beleid gecategoriseerd als landen met een zeer verhoogd kennisveiligheidsrisico.

2. De Academic Freedom Index[9] als indicator voor mogelijk misbruik van kennis en/of schending van de academische waarden. In de Nationale Leidraad Kennisveiligheid worden landen met een score van 0.40 of lager aangemerkt al risicolanden. Hier is een verhoogd risico op academische onderdrukking, censuur, beïnvloeding en misbruik van samenwerking. In dit beleid worden deze landen daarom aangemerkt als landen met een verhoogd kennisveiligheidsrisico.

3. Specifieke wet- en regelgeving van landen rond data-toegang, encryptie, exportcontrole en toezicht, in combinatie met actuele politieke of maatschappelijke ontwikkelingen. Wanneer dergelijke factoren de kennisveiligheid kunnen beïnvloeden, bepalen de Adviesgroep Kennisveiligheid en de CISO per geval wat het risico is. Deze landen worden in dit beleid aangemerkt als landen met een *tijdelijk* verhoogd kennisveiligheidsrisico.

Op basis van deze bronnen zijn de onderstaande risicocategorieën vastgesteld. Deze categorieën zijn niet alleen relevant voor het land van bestemming, maar ook voor alle landen waarlangs wordt gereisd of waar een tussenstop/overstap plaatsvindt, omdat ook daar kennisveiligheidsrisico's kunnen optreden.

[5] https://www.nederlandwereldwijd.nl/reisadvies/kleurcode-per-land

[6] https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid

[7] https://assets-us-01.kc-usercontent.com/d8b6f1f5-816c-005b-1dc1-e363dd7ce9a5/1fa3ec01-6b56-4840-b36b-1dd4f188c814/Kader%20Kennisveiligheid%20VU.pdf

[8] https://www.aivd.nl/documenten/2025/07/17/dreigingsbeeld-statelijke-actoren-2025

[9] https://academic-freedom-index.net/

- **Categorie Rood**: Landen met een zeer verhoogd risico. Landen die een zeer groot risico vormen voor de kennisveiligheid vanwege offensieve cyberprogramma's en/of militaire dreiging, benoemd door de AIVD. In 2026 omvatten deze landen onder meer **China (incl. Hongkong)**, **Rusland**, **Noord-Korea** en **Iran**. De lijst met landen staat op de website kennisveiligheid[1], of kan opgevraagd worden bij de contactpersoon kennisveiligheid van jouw eenheid.
    - Het gebruik van een reislaptop en reistelefoon wordt **verplicht** voor alle reizen met dienstapparatuur naar deze landen. De bijbehorende voorbereidingsrichtlijnen (zie 4D), gedragsinstructies tijdens de reis (zie 5C) en nazorgprocedures na terugkomst (zie 6) zijn ook van toepassing.

- **Categorie Oranje**: Landen met een verhoogd risico. Landen die een groot risico vormen voor de kennisveiligheid vanwege misbruik van kennis en/of schending van academische waarden. In principe **alle landen met een score lager dan 0.4 op de Academic Freedom Index**[9]. Voorbeelden van landen die in 2026 hieronder vallen zijn **de Verenigde Staten, India**, **Oekraïne**, **Maleisië**, **Turkije** en **Egypte**. De lijst met landen staat op de website van kennisveiligheid[1], of kan opgevraagd worden bij de contactpersoon kennisveiligheid van jouw eenheid.
    - Het gebruik van een reislaptop en reistelefoon is de **standaard** voor alle reizen met dienstapparatuur naar deze landen. Als hiervan wordt afgeweken, moet worden gemotiveerd waarom reisapparatuur voor deze reis niet wordt ingezet. De bijbehorende voorbereidingsrichtlijnen (zie 4C), gedragsinstructies tijdens de reis (zie 5B) en nazorgprocedures na terugkomst (zie 6) zijn ook van toepassing.

- **Categorie Geel**: Landen met een tijdelijk verhoogd risico. Landen waarmee traditioneel een positieve relatie bestaat, kunnen **vanwege specifieke wet- en regelgeving, in relatie tot verschuivende politieke of maatschappelijke dynamieken**, aanleiding zijn om met extra aandacht te kijken naar mogelijke risico's op het gebied van kennisveiligheid. De volledige en actuele lijst met landen staat op de website van kennisveiligheid[1], of kan opgevraagd worden bij de contactpersoon kennisveiligheid van jouw eenheid.
    - Het gebruik van een reislaptop en reistelefoon is de **standaard** voor alle reizen met dienstapparatuur naar deze landen. Als hiervan wordt afgeweken, moet worden gemotiveerd waarom reisapparatuur voor deze reis niet wordt ingezet. De bijbehorende voorbereidingsrichtlijnen (zie 4C), gedragsinstructies tijdens de reis (zie 5B) en nazorgprocedures na terugkomst zijn ook van toepassing.

- **Categorie Groen**: Landen zonder verhoogde dreiging op het gebied van kennisveiligheid of informatiebeveiliging. Ondanks dat dit veilige landen zijn, gelden hier ook de basisprincipes voor digitale- en kennisveiligheid.
    - Er is geen noodzaak voor het gebruik van een reislaptop en reistelefoon, wel gelden de basisregels voor kennisveiligheid en informatiebeveiliging bij de voorbereiding op de dienstreis (zie 4B) en tijdens de dienstreis (zie 5A). Mocht je toch een reisapparaat mee willen nemen, contacteer de contactpersoon kennisveiligheid van jouw eenheid.

NB: Het risicoprofiel van een land voor kennisveiligheid en informatiebeveiliging kan als gevolg van geopolitieke ontwikkelingen wijzigen. **Het is daarom altijd van belang om bij de planning van een reis naar de laatst beoordeelde situatie te kijken.** Raadpleeg de website kennisveiligheid, de contactpersoon kennisveiligheid en/of centraal informatie beveiliger van jouw eenheid is, bij twijfel contacteer de adviesgroep kennisveiligheid via kennisveiligheid@vu.nl.

Aanvullende risico inschatting

Naast het risicoprofiel van het land speelt ook **wat jij in jouw functie doet** en **hoe kwetsbaar de kennis en informatie is waarmee je werkt**, een belangrijke rol bij de risico-inschatting. Volgens het Kader Kennisveiligheid[1] gaat het daarbij onder meer om drie factoren:

- **Dual-use kennis of technologie**: kennis die zowel een civiele als een militaire toepassing kan hebben;
- **Sensitieve kennis- of technologiegebieden**: zoals sleuteltechnologieën of emerging technologies die door de overheid als strategisch worden gezien;
- **Ethische kwesties**: bijvoorbeeld risico's op mensenrechtenschendingen, repressie of onbedoelde kennisoverdracht.

Ook in landen met een *groen* of *geel* risicoprofiel kunnen deze factoren betekenen dat extra maatregelen of opschaling nodig is in het proces. Denk bijvoorbeeld aan:

- Onderzoek naar algoritmen die ook voor surveillancesystemen gebruikt kunnen worden (dual-use);
- Samenwerking rond geavanceerde labtechnieken of biotechnologie (sensitief domein);
- Het delen van data over kwetsbare of gemarginaliseerde groepen (ethisch risico).

Daarnaast kan jouw eigen functie of toegangsniveau het risico verhogen. Medewerkers met uitgebreide autorisaties, toegang tot grote hoeveelheden persoonsgegevens of die werken met afgeschermde onderzoeksopstellingen, moeten extra alert zijn. Denk bijvoorbeeld aan:

- Medewerkers met brede toegang tot HR-systemen: bijvoorbeeld toegang tot personeels- en studentendossiers, salarisgegevens en andere vertrouwelijke persoonsgegevens;
- Leidinggevenden of bestuurders met sensitieve organisatie-informatie: zoals strategische plannen, financiële gegevens of interne besluitvorming;
- Klinische onderzoekers met toegang tot medische dossiers: waaronder patiëntgegevens en onderzoeksdata met een hoge mate van vertrouwelijkheid.

In zulke gevallen kunnen aanvullende maatregelen nodig zijn, zelfs wanneer het bestemmings- of doorreisland een lager risicoprofiel heeft. Het Kader Kennisveiligheid biedt hiervoor handvatten en aandachtspunten voor risicoherkenning. Je contactpersoon kennisveiligheid kan helpen bij het maken van een onderbouwde risico-inschatting en het bepalen van passende maatregelen. In sommige situaties kan het bijvoorbeeld verstandig zijn om met een reislaptop te reizen, zodat gevoelige data en systemen goed zijn afgeschermd.

4. Voorbereiding op reis met dienstapparatuur

Je hebt zelf een belangrijke rol in het zorgvuldig omgaan met gevoelige informatie. De VU zorgt daarbij voor passende ondersteunende middelen en biedt advies op het gebied van kennisveiligheid en informatiebeveiliging. In het algemeen geldt dat er zo min mogelijk vertrouwelijke gegevens meegenomen moeten worden op een dienstreis. Stel jezelf daarom altijd de volgende vragen:

- Welke apparaten neem ik mee? Heb ik deze apparaten, applicaties en informatie écht nodig tijdens mijn reis?
- Wat is de waarde van de informatie die ik meeneem en/of online raadpleeg (denk ook aan informatie op papier, op gegevensdragers of anderszins)?
- Ga uit van een worst-case scenario: hoe erg zou het zijn als alle meegebrachte informatie in de verkeerde handen valt (inclusief alle wachtwoorden die ooit op het systeem zijn ingevoerd)?

Neem je toch sensitieve of vertrouwelijke gegevens mee, zoals onderzoeksdata over bijvoorbeeld sensitieve technologieën of privacygevoelige gegevens, neem dan contact op met de contactpersoon kennisveiligheid van jouw eenheid. Zij kunnen (samen met de centraal informatie beveiliger) adviseren over hoe dit op een zo veilige manier kan. Voor hulp bij de beveiliging hiervan kan er contact gezocht worden met het Security en Privacy Team (zie onder ‘Belangrijke Contacten’).

Stel ook een lijst op met de documenten, gegevensdragers en apparatuur die je meeneemt. Zo is bij verlies meteen duidelijk wat er weg is. Neem deze lijst niet mee op reis, maar bewaar deze op kantoor. Vervoer ook altijd alle vertrouwelijke documenten in de handbagage en niet in de check-in bagage.

De voorbereiding voor een dienstreis verschilt per land. Deze voorbereiding is gebaseerd op de vastgestelde risicocategorieën en geldt niet alleen voor het land van aankomst, maar ook voor landen waar je doorheen reist of een tussenstop maakt. Hieronder is een overzicht van de risico’s en de bijbehorende maatregelen om gegevens en apparatuur te beschermen. **De maatregelen zijn cumulatief: bij een hoger risicoprofiel land, blijven de maatregelen uit de lagere categorieën van kracht, aangevuld met extra maatregelen. Dus alle maatregelen die gelden voor land of gebied met een veilig risicoprofiel, gelden ook voor land of gebied met een verhoogd risicoprofiel (geel of oranje). Voor landen met een zeer verhoogd risicoprofiel (rood) gelden alle maatregelen.**

A. Privéreizen en privé apparatuur tijdens reizen met dienstapparatuur

Privéreizen met dienstapparatuur

Tijdens privéreizen moet zo min mogelijk zakelijke informatie en gegevensdragers mee worden genomen. Dit vermindert het risico op verlies, diefstal of beschadiging van apparatuur de VU. Tijdens privéreizen buiten de EU mag geen VU-apparatuur worden meegenomen, met uitzondering van de mobiele telefoon indien deze ook privé wordt gebruikt. Als de telefoon wordt meegenomen, dient het risicoprofiel van de bestemmings- en doorreislanden te worden gecontroleerd en overeenkomstige maatregelen te worden genomen.

Privé-apparatuur tijdens dienstreizen

Het gebruik van privé-apparatuur voor werk gerelateerde zaken tijdens dienstreizen is niet toegestaan in landen met een **rood** risicoprofiel. Deze beperking heeft als doel het risico op een datalek en kennisverlies te beperken. Wanneer privé-apparatuur toch noodzakelijk is bij reizen naar landen met een geel of oranje risicoprofiel (bijvoorbeeld voor privégebruik), gelden aanvullende voorzorgsmaatregelen om kruisbestuiving tussen privé- en werkgegevens te voorkomen:

- Log uit bij al je werk gerelateerde accounts en gebruik deze niet meer. Denk hierbij aan Outlook, Teams, OneDrive etc;
- Wis eventueel aanwezige VU-gegevens, -bestanden en -koppelingen, dus ook je VU mail, agenda en contacten op je privé telefoon.

B. Voorbereiding bij een dienstreis naar een land met een Groen risicoprofiel

In deze landen hebben een vergelijkbaar risicoprofiel als Nederland en gelden dus vergelijkbare maatregelen.

- Je laptop, tablet, gegevensdrager of telefoon kan tijdens de reis stukgaan, kwijtraken of gestolen worden. Daarom moet je dit regelen:
  - Gebruik standaardapparatuur van de VU, want deze is beheerd en beveiligd met een sterk wachtwoord. Ook is de opslag versleuteld, hebben de apparaten automatische schermvergrendeling en zijn ze te wissen op afstand;
  - Gebruik verschillende wachtwoorden voor al je accounts en zorg ervoor dat deze niet hetzelfde zijn als je VU-inloggegevens;
  - Bewaar je gegevens op een veilige locatie in de VU OneDrive, Teams, SharePoint of onderzoeksomgeving zoals Research Drive;
  - Zorg dat je de contactgegevens van de IT-servicedesk, Security and Operations Control Center (zie onder ‘Belangrijke Contacten’) en verzekeraars bij je hebt, zowel digitaal als op papier. Bewaar ze op een veilige plek zodat je meteen hulp kan inschakelen wanneer nodig.

- Je apparatuur of gegevens kunnen worden gehackt. Criminelen kunnen je gegevens stelen of versleutelen via kwaadaardige software. Daarom moet je dit regelen:
  - Gebruik standaardapparatuur van de VU, want deze is beheerd en beveiligd met een sterk wachtwoord. Ook is de opslag versleuteld en is er een backup van de gegevens. Daarnaast hebben de apparaten automatische schermvergrendeling en zijn ze te wissen op afstand.

C. Voorbereiding bij een dienstreis naar een land met een Geel of Oranje risicoprofiel

Het reizen naar landen of gebieden met een verhoogd risicoprofiel kan extra risico’s met zich meebrengen. Daarom moet je bij reizen naar deze landen of gebieden, naast de bovengenoemde voorbereidingen, ook de volgende risico’s en maatregelen in acht nemen.

- Je conversaties of gegevens kunnen worden afgetapt. Daarom moet je dit regelen:

    - Voer telefoongesprekken alleen over een end-to-end versleutelde verbinding met een app als Teams of Signal. Download en installeer deze apps van tevoren en zorg dat de benodigde contacten zijn toegevoegd. Zie de intranetpagina van informatiebeveiliging over welke (vertrouwelijke) gesprekken je met welke applicatie mag voeren.
    - Het gebruik van externe opslagmedia (zoals USB-sticks of externe schijven) wordt afgeraden. Indien gebruik noodzakelijk is, dient de data te worden versleuteld conform de geldende beveiligingsrichtlijnen.

- Voor landen in categorie **Oranje** en **Geel** is het gebruik van een lege VU-reislaptop en -reistelefoon de standaard. Als hiervan wordt afgeweken, moet bij de contactpersoon kennisveiligheid en de leidinggevende worden gemotiveerd waarom deze apparatuur niet wordt ingezet. Omdat de specifieke risico's kunnen variëren per situatie, wordt medewerkers verzocht om in overleg met de contactpersoon kennisveiligheid te bepalen welke maatregelen passend zijn. De reisapparaten kunnen worden aangevraagd via het IT-service portal [LINK]. Doe dit op tijd, zodat zij in overleg met jou de juiste diensten en beveiligingsmaatregelen kunnen installeren. Voor instructies over het gebruik van de reislaptop zie Bijlage 1. Voor het gebruik van reistelefoon in de installatie van een eSIM nodig, deze moet besteld worden via HolaFly zodat er voldaan wordt aan de Europese telecomrichtlijnen en standaarden. Voor een gedetailleerde bestel instructie, zie Bijlage 2.

- Mocht in samenspraak met de contactpersoon Kennisveiligheid van de eenheid worden besloten dat er geen reisapparaten worden meegenomen en dat de reguliere VU-laptop meegaat, dan is het belangrijk om hiervan de mogelijke gevolgen te kennen. Je apparatuur kan verplicht worden gecontroleerd door autoriteiten (aan de grens), waar zij jouw apparatuur kunnen uitlezen en/of kopiëren. Daarom moet je de volgende stappen volgen:
    - Schakel gebruik van biometrische toegang tot de apparatuur uit en gebruik sterke wachtwoorden;
    - Schakel de bluetoothfunctie van je telefoon en laptop uit en verbind niet met onbekende apparatuur. Bluetooth kan onveilig zijn, spionage via deze functie is uiterst eenvoudig. Gebruik (rand)apparatuur met een draad;
    - Minimaliseer de belgeschiedenis van je telefoon, verwijder ontvangen en verzonden sms-berichten en zet alleen noodzakelijke contacten in je contactenlijst;
    - Minimaliseer de hoeveelheid gevoelige gegevens en de accounts die je meeneemt tot het hoogstnoodzakelijke om de toegang ertoe zoveel mogelijk te beperken;
    - Schakel de locatieservices op je telefoon standaard uit en gebruik deze alleen als je deze echt nodig hebt.

D. Voorbereiding bij een dienstreis naar een land met een **Rood** risicoprofiel

Het reizen naar landen met een zeer verhoogd risicoprofiel brengt extra risico's met zich mee, zoals verplichte inlevering van apparatuur aan autoriteiten, spionage, chantage of afpersing. Naast alle bovenstaande maatregelen, kunnen de volgende maatregelen worden getroffen in overleg met de contactpersoon van kennisveiligheid van de faculteit of dienst:

- Neem een VU-reistelefoon en -laptop mee en laat je eigen apparatuur thuis. Een reislaptop en -telefoon kan je regelen via het IT-service portal[10]. Doe dit minimaal vier weken van tevoren, zodat zij in overleg met jou de juiste diensten en beveiligingsmaatregelen kunnen installeren.
- Zorg ervoor dat de **authenticatie-app** die wordt gebruikt voor het inloggen op het VU-account wordt overgezet naar de reistelefoon, zodat toegang tot het account tijdens de reis geborgd blijft.
- Houd er rekening mee dat het aanbevolen is om na afloop van de reis de wachtwoorden van VU-accounts te wijzigen.
- Lees je in over het gebruik van de reisapparaten voor vertrek en raak bekend met de tekortkomingen van het apparaat voor vertrek, zodat je niet voor onverwachte verrassingen komt te staan. Voor instructies over het gebruik van de reislaptop zie Bijlage 1. Voor het gebruik van reistelefoon in de installatie van een eSIM nodig, deze moet besteld worden via HolaFly zodat er voldaan wordt aan de Europese telecomrichtlijnen en standaarden. Voor een gedetailleerde bestel instructie, zie Bijlage 2.

N.B.: Voor reizen naar China ontvangt de medewerker twee telefoons. Eén telefoon wordt gebruikt voor de hotspot, de authenticatie-app en end-to-end encrypted communicatie (Whatsapp en Signal), zoals hierboven beschreven. De tweede telefoon is bedoeld voor het gebruik van betalingsapps zoals WeChat en AliPay.

In China is het in de praktijk vaak niet mogelijk om op andere manieren te betalen, terwijl deze apps tegelijkertijd een verhoogd veiligheidsrisico met zich meebrengen. Om dit risico te beperken, wordt hiervoor een voormalig toestel van een medewerker ingezet dat niet langer geschikt is voor regulier gebruik.

Tijdens de dienstreis

A. Dienstreis naar een land met een **Groen** risicoprofiel

- Je apparatuur of gegevens worden gehackt. Criminelen kunnen vertrouwelijke informatie stelen of versleutelen door middel van kwaadaardige software of misbruik van onveilige netwerken. Om dit risico te beperken, volg je de volgende stappen:
  - Gebruik bij voorkeur VU-mail voor werk gerelateerde mail en wees extra alert met andere mailaccounts; klik/ open bijlagen alleen als je de afzender/verzoek kunt verifiëren;
  - Gebruik alleen versleutelde verbindingen én controleer de URL/afzender; download geen software/bestanden uit onbetrouwbare bron;
  - Verbind alleen met WiFi netwerken waarvan je kunt vaststellen wie het netwerk beheert, zoals een persoonlijk hotspot, een netwerk van de eigen organisatie, een netwerk waarvoor je persoonlijk inloggegevens hebt ontvangen of Eduroam;
  - Vermijd het gebruik van openbare of onbeveiligde Wi-Fi-netwerken (zoals gratis Wi-Fi op luchthavens, in cafés of hotels). Indien gebruik daarvan onvermijdelijk is, maak dan altijd gebruik van een actieve VPN-verbinding;

[10] https://services.vu.nl/

- Houdt er rekening mee dat een VPN het risico aanzienlijk verlaagt, maar een onbetrouwbaar netwerk niet volledig veilig maakt. Wees daarom extra alert bij het gebruik van openbare netwerken.

- Er kan ongewenst hardware of software aan je apparatuur worden toegevoegd, waarmee je apparatuur gemanipuleerd kan worden. Daarom moet je de volgende stappen volgen:
  - Installeer geen software uit onbekende bronnen;
  - Gebruik geen vreemde gegevensdragers (USB-sticks, SD-kaarten of harddrives).

- Op reis kunnen andere mensen bewust of onbewust meeluisteren en meekijken. Onbevoegde personen kunnen die informatie misbruiken. Daarom moet je dit regelen:
  - Gebruik een privacy-scherm op je laptop in publieke ruimtes;
  - Bespreek geen gevoelige kwesties in publieke ruimtes.

B. Dienstreis in een land met een Geel of Oranje risicoprofiel

- Conversaties of gegevens kunnen worden afgetapt. Daarom moet je de volgende stappen nemen:
  - Gebruik EduVPN (of VU-goedgekeurde VPN) bij voorkeur altijd bij internettoegang in geel/oranje, en verplicht op publieke of onbekende netwerken;
  - Vermijd openbare wifi, gebruik alleen beveiligde vertrouwde netwerken;
  - Log met je VU-account nooit in op een werkplek of apparaat dat niet van jou is;
  - Vermijd het bespreken van gevoelige onderwerpen aan de telefoon en in publieke ruimtes zoals een vliegtuig, trein, taxi of andere openbare ruimtes.

- Je kunt (online) geïntimideerd of bedreigd worden. Daarom moet je de volgende stappen nemen:
  - Wees alert op ‘toevallige’ ontmoetingen met personen die veel belangstelling hebben voor je werk of je privéleven;
  - Verstrek selectief informatie. Vertel contacten niet meer dan noodzakelijk, ook niet tijdens congressen of bijeenkomsten waar je spreekt;
  - Wees je ervan bewust dat mensen je kunnen filmen of geluidsopnames kunnen maken om je later onder druk te zetten. Beperk online delen van gevoelige informatie en posten op social media; gebruik de privacy-instellingen van sociale mediakanalen voor het beperkt delen van persoonsgegevens. Dat geldt zeker bij het gebruik van datingapps.

- In landen of gebieden met een verhoogd risico, is het mogelijk dat je apparatuur verplicht gecontroleerd wordt door autoriteiten. Ook bestaat de kans op actief monitoren van jouw elektronische communicatiesystemen, moet je ook de volgende stappen volgen:
  - Neem vertrouwelijke informatie en gegevensdragers altijd mee in je handbagage en niet in je koffer. Het gebruik van externe opslagmedia dient zoveel mogelijk te worden vermeden. Indien dit niet mogelijk is, moet de opgeslagen informatie worden beveiligd door middel van encryptie;
  - Laat je apparatuur en gegevens(dragers) niet onbewaakt achter. Hotelkluizen zijn geen veilige opslag;
  - Plaats je eigen externe opslagmedia niet in de apparatuur van derden, om te voorkomen dat deze besmet raakt met malware;

- Schakel de locatieservices op je telefoon alleen in als je deze nodig hebt.
- Gebruik alleen door de VU goedgekeurde opslag- en uitwisseldiensten (bijv. OneDrive/Teams/SharePoint/ResearchDrive); gebruik **geen** niet-goedgekeurde clouddiensten voor werkdata (o.a. Dropbox, WeTransfer, Google Drive, etc.);
- Vermijd het werken in openbare ruimtes en gebruik geen publieke computers, bijvoorbeeld in hotellobby's;
- Vergrendel apparaten altijd en zet ze uit bij langere tijd niet gebruiken en bij risicomomenten (bijv. grenscontrole/ onverwachte inspectie);
- Neem eigen opladers en adapters mee en gebruik geen vreemde apparaten en kabels.

C. Dienstreis in een land met een met een **Rood** risicoprofiel

Om de reisapparaten correct te gebruiken en daarmee de risico's op ongewenste overdracht van kennis en informatie te verkleinen, dienen de VU-reisapparaten zorgvuldig gebruikt te worden. Ondanks dat de reisapparaten beperkingen hebben, kunnen er wel degelijk risico's zijn bij verkeerd gebruik. Voor de uitgebreid gebruiksaanwijzing van de reislaptop, zie Bijlage 1.

- Gebruik bij voorkeur **mobiele data of de hotspot van de reistelefoon** in plaats van openbare (wifi)netwerken. Openbare wifi is eenvoudig te manipuleren en vormt daarmee een aanzienlijk risico. Schakel vliegtuigmodus in op zowel de telefoon als de laptop uit wanneer je deze niet gebruikt;
- Zorg ervoor dat de VPN is ingeschakeld op het apparaat dat het internetverkeer verstuurt. Dat betekent dat EduVPN actief moet zijn op de telefoon wanneer deze als hotspot wordt gebruikt, én dat EduVPN op de laptop na het verbinden met de hotspot of netwerk wordt ingeschakeld;
- EduVPN wordt op wifi-netwerken regelmatig geblokkeerd. Gebruik daarom altijd de VPN-verbinding via een mobiele-hotspot.
- Maak zo min mogelijk verbinding met VU-systemen; maak alleen gebruik van VU-diensten via je webbrowser. Het installeren van nieuwe applicaties is niet mogelijk en koppel je VU-mail account niet aan geïnstalleerde applicaties;
- De reislaptop is zo ingericht dat browserdata automatisch wordt gewist bij afsluiten. Zorg er daarom voor dat na het inloggen en gebruik van VU-diensten via je webbrowser, je de webbrowser sluit. Dit zorgt ervoor dat alle wachtwoorden en geschiedenis verwijderd wordt. Doe dit ook voor het dichtklappen van de laptop, anders blijven de diensten toegankelijk bij het openen van de laptop;
- Laat je laptop, telefoon of andere elektronische apparaten nooit onbeheerd achter. Vergrendel deze altijd als je er niet op aan het werk bent en zet uit als ze niet worden gebruikt voor langere tijd. Verbind de reisapparaten nooit met onbekende kabels, printers, opladers, gegevensdragers;
- Zorg ervoor dat de gegevens die je verwerkt geanonimiseerd zijn wanneer mogelijk.
- Laat jouw reisapparaten niet achter op een plaats waar anderen ze kunnen inzien. Dit geldt ook voor je hotelkamer of hotelkluis;
- Schakel apparaten uit tijdens vertrouwelijke gesprekken en leg ze buiten gehoorafstand. Zo verklein je de kans dat gesprekken kunnen worden gevolgd als een apparaat is geïnfiltreerd.

Indien bij aankomst een USB-stick (of een kabel/gegevensdrager) in je laptop wordt geplaatst of je laptop wordt aangesloten op een ander systeem, moet je de laptop als gecompromitteerd beschouwen. Dit geldt ook wanneer je verplicht wordt om applicaties te downloaden of te installeren in de bestemmings- en doorreislanden. Gebruik de laptop vanaf dat moment niet meer voor VU-werkzaamheden en maak gedurende de reis absoluut geen verbinding met VU-netwerken of (cloud)applicaties.

Beschouw dit als een incident: verbreek direct de verbinding, stop elk gebruik voor VU-doeleinden, meld het onmiddellijk bij het SOC/IT-servicedesk, én lever de apparatuur in voor controle.

5. Na afloop van de dienstreis

Bij terugkomst is het belangrijk om direct aandacht te besteden aan de beveiliging van zowel apparatuur als accounts. Wijzig zo snel mogelijk de toegangscodes van je apparaten (zoals pincode of ontgrendelwachtwoord, wanneer relevant). Pas daarna de wachtwoorden aan van alle gebruikte accounts, waaronder e-mail, cloudomgevingen en sociale-media-accounts, en trek actieve sessies in of log overal uit om mogelijk misbruik te voorkomen.

Lever de reisapparaten zo snel mogelijk in bij de IT Servicedesk zodat deze kunnen worden geanalyseerd, opgeschoond en klaargemaakt voor gebruik door een volgende medewerker. Laat daarnaast ook andere gebruikte VU-apparatuur, of apparatuur die tijdens de reis toegang had tot VU-accounts of gevoelige data, controleren op mogelijke beveiligingsinbreuken. Wijzig daarbij ook de relevante wachtwoorden en trek sessies in, zoals hierboven beschreven, om zeker te zijn dat accounts veilig blijven.

Bij mogelijke incidenten rondom informatiebeveiliging, zoals verlies of diefstal van apparatuur, malware, of een gecompromitteerd account, neem onmiddellijk contact op met de IT Servicedesk. Bij incidenten die een risico vormen voor kennisveiligheid, zoals benadering, druk of beïnvloeding, neem je direct contact op met de contactpersoon Kennisveiligheid.

Voordat je reisapparaten inlevert, moet je tijdelijke bestanden verwijderen of archiveren als er géén vermoeden van een incident is. Bij twijfel: niets wissen en eerst laten controleren. Als je ook maar enig vermoeden hebt dat er iets is voorgevallen, verbind de reisapparaten niet met VU-netwerken of je thuisnetwerk totdat deze gecontroleerd zijn. Zet het apparaat uit of laat het volledig offline, en neem direct contact op met de IT Servicedesk/SOC. Lever het apparaat vervolgens zo snel mogelijk in voor verdere analyse.

6. Belangrijke Contacten / Melden van Onveilige Situaties

Bij (vermoeden van) incidenten, verdachte berichten, onveilige ICT-situaties, gestolen of krijtgeraakte apparatuur of een (mogelijk) datalek, meld onmiddellijk bij de VU. Meld ook bij twijfel!

- Tijdens kantooruren (NL) bij de **IT Servicedesk** van VU Amsterdam
  E-mail: servicedesk.it@vu.nl
  Tel: +3120 59 80000
- Voor noodgevallen buiten kantooruren (NL) bij het **Security and Operations Control Center** van VU Amsterdam: Tel: +31 20 598 22 22

- **Informatiebeveiliging Support Desk**
  E-mail: infosec.is.it@vu.nl

Bijlage 1. Uitleg en gebruik Reislaptop

De reislaptop is bewust sterk beperkt ingericht om de digitale veiligheid tijdens reizen naar risicolanden te waarborgen. Hierdoor werkt het apparaat anders dan een reguliere VU-laptop en zijn verschillende functionaliteiten bewust uitgeschakeld.

De reislaptop bevat uitsluitend een lokaal gebruikersaccount; inloggen met een VU-netID of VU-mailadres is niet mogelijk. De beschikbare software is tot het minimum beperkt: alleen Word, Excel, PowerPoint en OneNote zijn lokaal geïnstalleerd. Andere Microsoft-diensten, zoals Outlook, OneDrive en Teams, kunnen uitsluitend via de webbrowser worden gebruikt. Het installeren van nieuwe applicaties via internet of via de Windows Store is geblokkeerd om misbruik en ongewenste software-installaties te voorkomen.

Ook de aansluitmogelijkheden zijn beperkt. Draadloze verbindingen zoals Bluetooth, Miracast en koppelingen met printers of andere randapparatuur zijn uitgeschakeld, waardoor het apparaat niet kan worden verbonden met externe hardware. Bestanden worden uitsluitend lokaal opgeslagen op de versleutelde schijf, omdat synchronisatie met cloudopslagdiensten zoals OneDrive en SharePoint is uitgeschakeld om datalekken te voorkomen. De webbrowser slaat geen geschiedenis, wachtwoorden of sessie-informatie op; zodra de browser wordt afgesloten, wordt alle tijdelijke data automatisch verwijderd. Daardoor blijven diensten alleen toegankelijk zolang de browser actief is.

Gebruikers beschikken bovendien niet over beheerrechten op de laptop en kunnen geen instellingen wijzigen die invloed hebben op de beveiliging of configuratie van het apparaat. Deze combinatie van maatregelen zorgt ervoor dat de reislaptop alleen de strikt noodzakelijke functionaliteit biedt om documenten te lezen of te bewerken en om via de browser beperkte toegang te krijgen tot VU-diensten. Toegang tot lokale apps, automatische synchronisatie en installatie-mogelijkheden is bewust uitgesloten. Dankzij deze opzet kan de reislaptop veilig worden gebruikt in digitale hoog-risico omgevingen, met minimale blootstelling aan spionagerisico's, interceptie of datalekken.

1. Aanvraag

Bespreek de risico's van de bestemmings- en doorreislanden met het contactpersoon kennisveiligheid en vraag de reisapparaten aan via de IT-webpagina[11].

2. Opstarten

Stel samen met IT een nieuw wachtwoord in voor het guest-account. Zorg ervoor dat dit wachtwoord anders is dan het wachtwoord van jouw VU-account. Dit wachtwoord zal vanaf nu toegang geven tot het guest-account, dus zorg ervoor dat je jouw wachtwoord zorgvuldig kiest en goed onthoudt.

3. Voorbereiding

Bedenk ook welke documenten je écht nodig hebt tijdens je reis, zodat je deze klaar kan zetten op OneDrive en ze bij aankomst makkelijk kan downloaden via de webbrowser.

Zorg ervoor dat de authenticator-app die wordt gebruikt voor het inloggen op het VU-account wordt overgezet naar de reistelefoon, zodat toegang tot het account tijdens de reis geborgd blijft.

[11] https://services.vu.nl/

4. Websites voor reizen

Email: https://outlook.com

OneDrive: https://onedrive.live.com/

Teams: https://teams.microsoft.com/

5. Voor de douane

Houd er rekening mee dat het mogelijk is dat je apparatuur verplicht gecontroleerd wordt door autoriteiten en dat je gevraagd wordt om in te loggen. Zorg er daarom voor dat alle (browser) vensters afgesloten zijn voor het passeren van de douane, zodat bij het openen van de laptop er geen toegang is tot het VU-netwerk.

6. In het risicoland

Om de digitale- en kennisveiligheid te garanderen, houd rekening met de volgende basisprincipes:

- **Maak nooit gebruik van openbare WiFi-netwerken.** Verbind de laptop uitsluitend met het internet via de hotspot van de VU-reistelefoon. Zorg ervoor dat **EduVPN op de telefoon is ingeschakeld** voordat je de laptop met de hotspot verbindt. Schakel de WiFi-functie op zowel laptop als telefoon uit wanneer je geen internet nodig hebt.
- **Beperk het gebruik van VU-systemen tot het noodzakelijke.** Gebruik VU-diensten uitsluitend via de webbrowser en koppel je VU-mail niet aan lokale applicaties. Installeer geen apps, updates of plug-ins via internet, de Windows Store of andere bronnen.
- **Sluit de webbrowser altijd volledig af na het gebruik van VU-diensten.** Hiermee worden alle wachtwoorden, sessies en geschiedenis automatisch verwijderd. Doe dit voordat je de laptop dichtklapt; anders blijven diensten toegankelijk bij het opnieuw openen.
- **Gebruik geen onbekende kabels, USB-sticks, gegevensdragers, opladers, adapters, printers, dockingstations of andere randapparatuur.** Presentaties kun je het beste vooraf mailen aan de organisator zodat je kunt presenteren via de aanwezige apparatuur.
- **Laat de laptop, telefoon en andere reisapparaten nooit onbeheerd achter.** Dit geldt ook voor hotelkamers en hotelkluizen. Bewaar apparaten uit het zicht.
- **Vergrendel de laptop direct wanneer je niet actief werkt** en schakel hem uit wanneer je langere tijd geen gebruik maakt van het apparaat.
- **Werk alleen met geanonimiseerde gegevens**, wanneer dat mogelijk is, om te voorkomen dat gevoelige informatie op het apparaat aanwezig is.
- **Houd de laptop en telefoon uitgeschakeld tijdens vertrouwelijke gesprekken.** Indien mogelijk kun je de batterij verwijderen, of het apparaat in je tas of tussen kleding bewaren om geluid te dempen. Dit verkleint het risico dat gesprekken kunnen worden gevolgd als een apparaat gecompromitteerd zou zijn.
- **Gebruik de reislaptop uitsluitend voor werk gerelateerde taken** die noodzakelijk zijn tijdens de reis.
- **Meld verlies, diefstal of vermoedelijke compromittering onmiddellijk** bij de contactpersoon kennisveiligheid of de IT-servicedesk.

7. De terugreis

Houd er weer rekening mee dat het mogelijk is dat je apparatuur verplicht gecontroleerd wordt door autoriteiten en dat je gevraagd wordt om in te loggen. Zorg ervoor dat alle bestanden weer op OneDrive staan en dat alle bestanden lokaal verwijderd zijn. Leeg hiervoor ook de prullenbak. Zorg er ook voor dat alle (browser) vensters afgesloten zijn voor het passeren van de douane, zodat bij het openen van de laptop er geen toegang is tot het VU-netwerk.

8. Bij terugkomst

Na terugkeer is het van belang om de reisapparaten zo snel mogelijk in te leveren bij de IT Servicedesk voor analyse en opschoning, andere gebruikte apparatuur te laten controleren op mogelijke beveiligingsinbreuken, en eventuele incidenten of bedreigingen voor kennisveiligheid te melden bij de contactpersoon kennisveiligheid. Zorg ervoor dat er geen bestanden meer lokaal aanwezig zijn, aangezien alles gewist wordt. Als je ook maar een vermoeden hebt dat er iets is voorgevallen, verbind de reisapparaten dan niet met een netwerk van de VU of met een thuisnetwerk totdat er een controle heeft plaatsgevonden.

Bijlage 2. Bestellen en installeren van de eSIM

1. Ga naar de website van Holafly

- Ga naar: https://esim.holafly.com/nl/
- Selecteer het land of landen waar je naartoe reist, en selecteer de reisdata.
- Klik op ‘Zoek bundel’.

2. Controleer de bestelling

- Controleer het aantal dagen van het abonnement en de reisdata.
- Klik op ‘Krijg onbeperkt internet’.
- Klink in het pop-up scherm ‘Ga naar afreken’.

3. Afrekenen

- Vul contactgegevens in, gebruik een emailadres die ook op reis gebruikt kan worden.
- Klik ‘Ga naar betalen’.
- Reken af met iDeal/Wero, Creditcard of PayPal.

4. Ontvangst van de eSIM

Na afronden van de bestelling ontvang je per e-mail:

- Een email met een factuur die gebruikt kan worden voor de declaratie.
- Een **QR-code** voor de eSIM met installatie-instructies van Holafly.

5. Installeer de eSIM op de reistelefoon

- Scan de QR-code onderaan de email met de camera-app van de iPhone.
- Er opent een melding met de vraag om een nieuwe e-sim te activeren.
- Klik op ‘Sta toe’.
- De eSIM wordt nu geinstalleerd, dit kan even duren.
- **Let op:** Installeer de eSIM bij voorkeur **voor vertrek**, maar activeer deze pas **op de reisbestemming.**

6. Activeer de eSIM **op de bestemming**

- Aangekomen op de bestemming, ga naar instellingen > mobiel netwerk.
- Scrol naar het kopje simkaarten en activeer de eSIM.
- Schakel eventueel dataroaming in voor de eSIM (indien gevraagd door het toestel).

7. Controleer de werking

- Test of internettoegang werkt (bijvoorbeeld door een webpagina te openen).