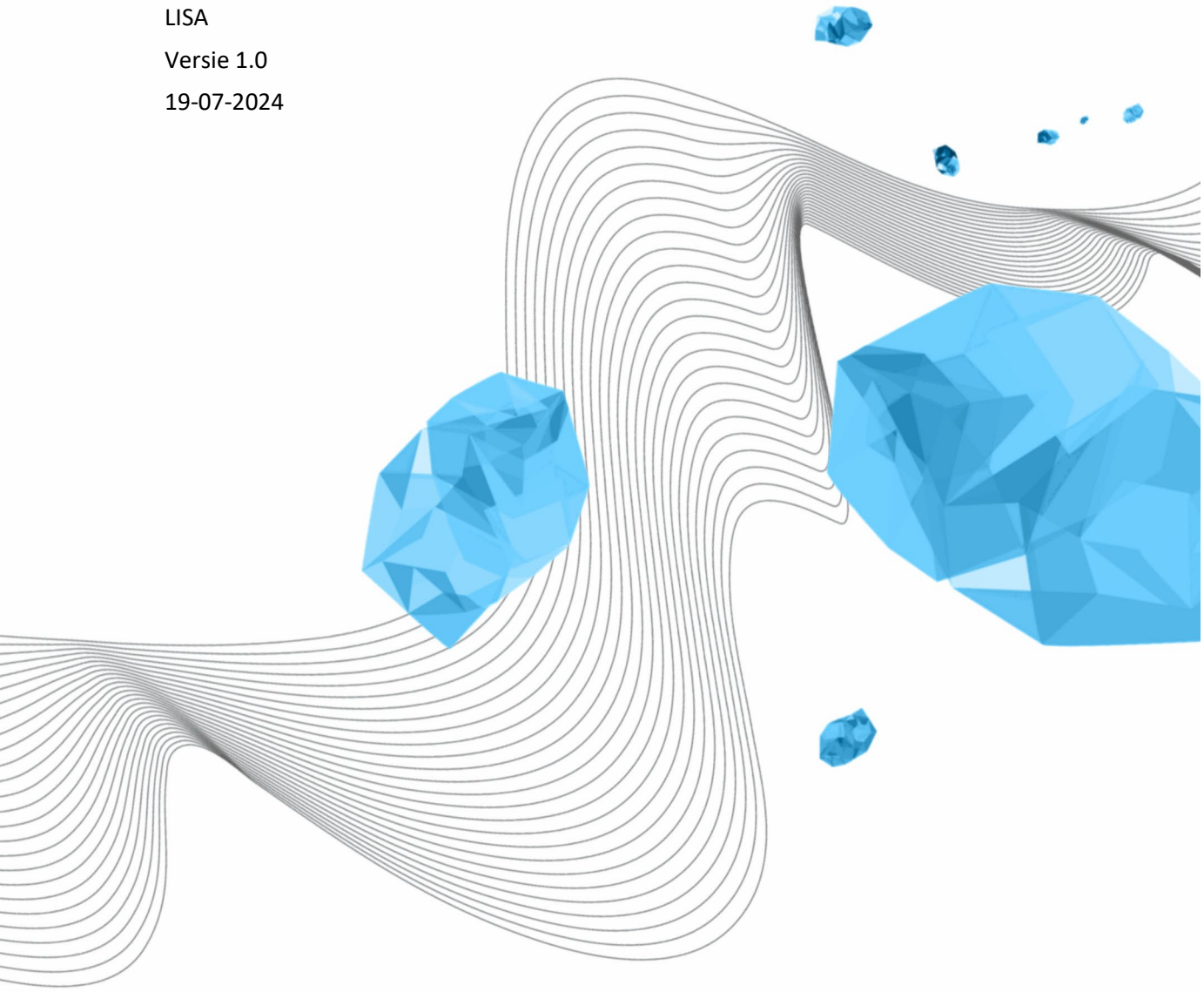
Status: Versie 1.0
Datum vastgesteld in CvB: 03-09-2024
Datum vastgesteld MT-LISA: 22-07-2024
Auteur: Henk Swaters

# KENNIS- EN INFORMATIEBEVEILIGING TIJDENS REIZEN NAAR HET BUITENLAND

LISA
Versie 1.0
19-07-2024



UNIVERSITY OF TWENTE.

# COLOFON

ORGANISATIE
Library, ICT Services & Archive

TITEL
Kennis- en informatiebeveiliging tijdens reizen naar het buitenland

KENMERK
LISA-0410

VERSIE (STATUS)
1.0

DATUM
19-07-2024

AUTEUR(S)
Henk Swaters



# DOCUMENTHISTORIE

| VERSIE | DATUM | AUTEUR(S) | OPMERKINGEN |
|---|---|---|---|
| 0.2 | 14-06-2024 | Henk Swaters | Eerste versie |
| 0.3 | 21-06-2024 | Henk Swaters | Feedback verwerkt |
| 0.4 | 25-06-2024 | Henk Swaters | Feedback verwerkt |
| 1.0 | 19-07-2024 | Henk Swaters | Toelichtingen op maatregelen toegevoegd |
| | | | |

# DISTRIBUTIELIJST

| VERSIE | DATUM | GEDISTRIBUEERD AAN | OPMERKING |
|---|---|---|---|
| 0.2 | 14-06-2024 | LISA security & kennisveiligheid | |
| 0.3 | 21-06-2024 | LISA security & kennisveiligheid | |
| 0.4 | 25-06-2024 | LISA security & kennisveiligheid & MT | |
| 1.0 | 22-07-2024 | LISA-MT | Vastgesteld |
| | | | |

# INHOUDSOPGAVE

# 1 INLEIDING

Ga je binnenkort voor je werk naar het buitenland? Zakelijke reizen naar het buitenland brengen spionagerisico's met zich mee. Ditzelfde geldt voor langdurig werkzaam zijn in het buitenland. Buitenlandse inlichtingendiensten en andere belanghebbenden hebben misschien interesse in jou en vooral in de kennis die je hebt of bij je draagt. Deze informatie helpt je bij het nemen van voorzorgsmaatregelen om het risico op (digitale) spionage te verkleinen.

De basis voor deze richtlijn is het document "Op reis naar het buitenland"[1] van de AIVD, waarbij er wat betreft maatregelen door de UT onderscheid is gemaakt tussen risicoprofielen. Als je een laag risicoprofiel hebt kunnen de maatregelen soms niet in verhouding staan tot de kosten. Om hier antwoord op te geven zijn de maatregelen aan een risicoprofiel gekoppeld. Indien je een midden- of hoogrisicoprofiel hebt, dan zijn de maatregelen van de lagere risicoprofielen ook van toepassing.

## 1.1 LEESWIJZER

In hoofdstuk 2 t/m 4 staan alle maatregelen voor alle risicoprofielen genoemd. In hoofdstuk 5 zijn de maatregelen aan een risicoprofiel gekoppeld, daarmee wordt het mogelijk om een aantal maatregelen te laten vallen als het risico dat toelaat om de kosten te drukken.

[1] https://www.aivd.nl/binaries/aivd_nl/documenten/publicaties/2017/12/20/op-reis-naar-het-buitenland/Brochure+Paspoort+Op+reis+naar+het+buitenland.pdf

# 2 VOOR DE REIS

## 2.1 ALGEMEEN

Neem geen of zo min mogelijk vertrouwelijke gegevens mee. Je bent zelf verantwoordelijk voor een zorgvuldige omgang met deze informatie. Stel jezelf voor vertrek daarom altijd de volgende vragen:

- Heb ik dit écht nodig?
- Wat is de waarde van de informatie die ik meeneem (op papier, een gegevensdrager of anderszins)?
- Hoe erg zou het zijn als de informatie in verkeerde handen valt?
- Welke apparaten neem ik mee?

Neem je toch vertrouwelijke gegevens mee, stel dan een lijst op met de documenten, gegevensdragers en apparatuur die je meeneemt. Bij verlies is dan meteen duidelijk wat er weg is. Bewaar de lijst op kantoor, neem deze niet mee. Vervoer jouw vertrouwelijke documenten en gegevensdragers altijd in jouw handbagage, nooit in jouw koffer.

Neem vooraf contact op met het Knowledge Safety Team (KST)[2] om te informeren of er speciale aandachtspunten zijn voor je reis. Doe dit altijd als je twijfelt of als je een hoogrisicoland bezoekt. Dit zijn op dit moment China, Iran, Rusland en Noord-Korea. Deze landen hebben een offensief digitaal aanvalsprogramma[3]. Dat wil overigens niet zeggen dat andere landen geen hoog risico kunnen vormen. Vraag ook naar de regels voor het vervoeren van (staats)geheime informatie, indien van toepassing.

Stem bezoeken aan overheidsorganisaties af met het Nederlandse consulaat of de ambassade, indien aanwezig.

[2] https://www.utwente.nl/en/service-portal/internationalisation-foreign-affairs/knowledge-safety-export-control
[3] AIVD, 2023, 'Beschouwing risico's gebruik applicaties uit landen met een offensief cyberprogramma gericht tegen Nederland'

## 2.2 DIGITAAL

Overweeg een wegwerp mobiele telefoon met zo min mogelijk gegevens en apps, een tijdelijke simkaart[4] en tijdelijk e-mailadres te gebruiken. Indien dat niet mogelijk is, wis dan vooraf de telefoon.

Installeer alleen applicaties die je daadwerkelijk nodig hebt en vermijd apps die problemen hebben met privacy of gegevensbeveiliging. Zorg ervoor dat je alleen noodzakelijke contacten in je contactenlijst hebt. Voor chatfunctionaliteit is Signal de meest veilige applicatie, ook al is deze minder populair dan WhatsApp, SMS of WeChat. Het is belangrijk om multi-factor authenticatie en sterke wachtwoorden te gebruiken, ook voor je Apps. Neem eventueel contact op met CERT-UT[5] voor advies.

Als je regelmatig naar het buitenland reist, is het raadzaam apparatuur aan te schaffen die je alleen voor dit doel gebruikt. Neem eigen opladers, adapters, kabels en carkit mee. Zorg ook dat je deze apparatuur op afstand kunt wissen, hoe dat werkt is vaak te vinden op de website van de smartphonefabrikant.

Als je voor de reis vooraf een SIM-kaart kaart met databundel koopt, denk dan goed na over de grote van de databundel. Tegenwoordig gebruik je snel 500Mb per dag, zelfs als je zuinig werkt. Koop geen SIM-kaart in een hoogrisicoland!

Als je de SIM kaart in een “veilig” land van bestemming koopt, doe dat alleen bij gerenomeerde winkels. Dus nooit bij straatverkoop. Hou er dan ook rekening mee dat je tegenwoordig vaak een eSIM krijgt en daarvoor moet je toestel geschikt zijn.

Pas wachtwoorden voor (en na) jouw reis aan.

Gebruik verschillende wachtwoorden voor al jouw apparaten en zorg ervoor dat die niet hetzelfde zijn als de inloggegevens van jouw werkplek.

Voorkom dat iemand meekijkt of ongemerkt aan jouw apparatuur rommelt. Je kunt jouw webcam afdekken, gebruikmaken van een privacyscherm of speciale anti-tamper stickers. Vanwege de grote diversiteit aan apparatuur is dit een maatwerkbestelling via afdeling Inkoop (CFM).

## 2.3 PRIVÉ

Wees terughoudend met het meenemen en gebruik van privéapparatuur. Ook die is interessant. Zorg dat je verschillende toestellen gebruikt voor jouw privégesprekken en jouw professionele gesprekken en houd deze zoveel mogelijk gescheiden.

Neem op een privéreis zo min mogelijk zakelijke informatie en gegevensdragers mee.

Zet niets op sociale media, zoals Twitter en Facebook, dat je op reis gaat.

[4] Bijvoorbeeld: https://reissim.nl/china-esim-simkaart-en-censuur/
[5] https://www.utwente.nl/nl/cyber-safety/meld-incidenten/

# 3 TIJDENS DE REIS

## 3.1 ALGEMEEN

Voer geen vertrouwelijke gesprekken aan de telefoon of in vervoersmiddelen zoals een huurauto, trein of vliegtuig. Houd informatie en gegevensdragers zoveel mogelijk bij je.

Vertel jouw gesprekspartner niet meer dan nodig is.

Wees alert op 'toevallige' ontmoetingen met personen die veel belangstelling hebben voor jouw werk of privéleven. Ook via sociale media kan geprobeerd worden met je in contact te komen.

Jouw gedrag kan je direct of op een later moment in een kwetsbare positie brengen. Niet alleen alcohol of drugs, ook geschenken of avances kunnen worden ingezet om je te beïnvloeden.

Wees je ervan bewust dat mensen je kunnen filmen of geluidsopnames kunnen maken om je later onder druk te zetten. Dat geldt zeker ook bij gebruik van sociale media of datingapps!

Zorg dat je kunt controleren of iemand vertrouwelijke gegevens heeft ingezien. Gebruik daar sealbags[6] voor.

Hoewel een hotelkluis beter is dan geen kluis, vormt ook deze een risico. Gebruik de hotelkluis bij voorkeur niet voor vertrouwelijke informatie of gegevensdragers. Houd deze spullen bij je. Als het niet anders kan, gebruik dan de kluis in de kamer of neem een klein reiskluisje mee. Deze kun je in je koffer meenemen en met een kabel ergens aan vastmaken in de hotelkamer.

## 3.2 DIGITAAL

Schakel jouw apparaten uit als je een vertrouwelijk gesprek voert. Verwijder (indien mogelijk) de batterij, of leg jouw apparaat tussen jouw kleding of in jouw tas zodat het geluid gedempt wordt. je bent extra kwetsbaar voor spionage als jouw apparatuur ingeschakeld is.

Schakel Wifi en de Bluetooth-functie van al jouw apparaten uit. Zie hiervoor de handleiding van je device. Bluetooth is onveilig en spionage via deze functie is uiterst eenvoudig. Schakel Wifi alleen in als dat nodig is.

Download of installeer geen applicaties tijdens de reis. Schakel automatische updates voor de App Store of Play Store uit tijdens het reizen. In onveilige landen kunnen namelijk nep-appstores worden aangeboden die malware bevatten. Zodra je terug bent in een veilig land moet je updates weer inschakelen.

Let op onverwachte of vreemde (beveiligings-) waarschuwingen op jouw telefoon, laptop of tablet. De meldingen kunnen wijzen op een aanval. Houd meldingen en andere opvallende zaken bij en geef deze door aan CERT-UT. Overleg dan ook of je de apparatuur nog kunt blijven gebruiken.

Geef nooit jouw wachtwoord af en sta niet toe dat anderen gebruik maken van jouw apparatuur of kabels.

Gebruik geen Wifi die wordt aangeboden in openbare ruimtes.

[6] Bijvoorbeeld: https://www.debatin.com/safebag-for-tablets-and-smartphones/

Wil je mobiel werken? Gebruik dan nooit apparatuur van derden. Sluit jouw systeem ook nooit aan op apparatuur van anderen (denk aan printers en opladers). Presentaties kun je beter van tevoren mailen aan persoon die je heeft uitgenodigd zodat je via de daar aanwezige computer kunt presenteren.

Wanneer je op reis bent, is het belangrijk om veilig te internetten. Gebruik hiervoor de "Secure Internet" optie van eduVPN[7]. Dit zorgt ervoor dat je internetverbinding versleuteld is en beschermt je gegevens tegen hackers.

Gebruik geen USB-sticks. Als het echt niet anders kan, gebruik dan alleen je eigen USB-stick van een betrouwbare fabrikant. Zorg ervoor dat je deze hebt versleuteld en veilig bewaart.

Gebruik ook geen USB-opladers en andere USB devices van anderen. Denk hierbij ook aan een eventuele USB aansluiting in een (huur)auto, ook deze kunnen gegevens overdragen. In noodgevallen kun je vooraf aan de reis een USB-blocker aanschaffen waarmee je alleen kunt opladen.

Wees terughoudend met het openen van e-mails, sms-berichten of andere elektronische berichten van onbekenden. Pas op voor spear phishing. Ga altijd na of ontvangen berichten voor je bestemd zijn. Bij twijfel verifieert je eerst de herkomst van het bericht bij de afzender.

Geef jouw apparatuur nooit af. Moet dat wel vanwege veiligheidsmaatregelen, stop ze dan in een sealbag[8] of geef ze aan een collega die niet met je mee naar binnen gaat.

Waarschuw bij een incident altijd direct CERT-UT. Doe dit ook bij twijfel!

# 4 NA DE REIS

## 4.1 ALGEMEEN

Verander het wachtwoord van de meegenomen apparatuur en van accounts, zoals e-mail en sociale media. Zet automatische updates weer aan. Het kan zijn dat jouw apparatuur ingeleverd moet worden voor analyse of opschoning. Soms kan het zelfs nodig zijn om apparatuur te vernietigen bij terugkomst, omdat veilig gebruik niet meer mogelijk is. Per reisbestemming en organisatie kunnen hier specifieke afspraken over bestaan, stem dit vooraf af met het Knowledge Safety Team[9].

Vreemden kunnen nog enige tijd na de reis contact opnemen en refereren aan gebeurtenissen en “vriendschappen” opgedaan tijdens de reis. Ga daar voorzichtig mee om

# 5 UITGANGSPUNTEN EN KADERS

## 5.1 INLEIDING

Zoals eerder gemeld is het verstandig om alle maatregelen te treffen voor, tijdens en na je reis, maar als je een laag risicoprofiel hebt kunnen de maatregelen soms niet in verhouding staan tot de kosten. Om hier antwoord op te geven zijn de maatregelen aan een risicoprofiel gekoppeld. Indien je een midden- of hoogrisicoprofiel hebt, dan zijn de maatregelen van de lagere risicoprofielen ook van toepassing

[7] https://www.eduvpn.org/ of https://utwente.nl/vpn
[8] Bijvoorbeeld: https://www.debatin.com/safebag-for-tablets-and-smartphones/
[9] https://www.utwente.nl/en/service-portal/internationalisation-foreign-affairs/knowledge-safety-export-control

Indien medewerkers tijdelijk in hun oorspronkelijke thuisland willen werken, bijvoorbeeld vanwege familieomstandigheden zoals zorgverplichtingen, is voorafgaande goedkeuring van hun leidinggevende vereist. Echter, buiten de EU is het nooit toegestaan om gebruik te maken van speciale autorisaties in bedrijfssystemen waarmee toegang bestaat tot gevoelige gegevens, zoals persoonsgegevens van anderen. Medewerker en leidinggevende moeten ervoor zorgen dat de autorisatie wordt ingetrokken indien de medewerker buiten de EU verblijft.

## 5.2 RISICOPROFIELEN

Het risico dat je loopt tijdens een reis is mede afhankelijk van de kennis en informatie die je bezit of waar je toegang toe hebt. Dus ook hoe strict je de maatregelen moet toepassen is hiervan afhankelijk. Bij voorkeur tref je alle maatregelen, maar soms kun je daar iets soepeler in zijn. De risicoprofielen die we onderscheiden zijn:

**Laag Risicoprofiel**

- Administratief personeel en ondersteunend personeel zonder toegang tot gevoelige onderzoeksgegevens of en niet geautoriseerd voor toegang tot bedrijfssystemen die toegang bieden tot andere gevoelige gegevens (zie 5.1).
- Studenten die deelnemen aan reguliere studies zonder betrokkenheid bij gevoelige onderzoeksprojecten.

**Midden Risicoprofiel**

- Onderzoekers die werken aan projecten met matig gevoelige informatie, zoals openbare onderzoeksprojecten of samenwerkingen met andere instellingen.
- Personeel met toegang tot interne beleidsdocumenten of strategische plannen.
- Administratief en ondersteunend personeel dat geautoriseerd is voor toegang tot bedrijfssystemen die inzage bieden in gevoelige bedrijfsgegevens of persoonsgegevens.

**Hoog Risicoprofiel**

- Hoogleraren en Promovendi die betrokken zijn bij onderzoek met hoge mate van vertrouwelijkheid of commerciële waarde.
- IT-Beheerders/functionarissen met hoge rechten of toegang tot gevoelige data en infrastructuur.
- Bestuursleden die strategische beslissingen nemen en toegang hebben tot gevoelige institutionele informatie.

- 

## 5.3 MAATREGELEN LAAG RISICOPROFIEL

- Neem alleen apparatuur mee die nodig is voor de reis.
- Stel een lijst op van documenten en apparatuur die wordt meegenomen. Bewaar die lijst thuis.
- Beperk de toegang tot gegevens tot alleen diegenen die het nodig hebben voor hun werk.
- Het is essentieel om sterke, unieke wachtwoorden te gebruiken voor alle ICT-diensten en indien nodig[10] regelmatig te veranderen. Dit omvat ook het gebruik van multi-factor authenticatie om toegang tot accounts extra te beveiligen, ook van je eigen social media accounts.
- Versleutel datadragers zoals de harddisk van je laptop en de opslag van je telefoon.
- Installeer en onderhoud betrouwbare antivirus- en antimalwareprogramma's op al je apparaten om ze te beschermen tegen schadelijke software.
- De managed werkplek van de UT heeft een antivirus- en antimalwareprogramma om deze computer te beschermen tegen schadelijke software.
- Volg de richtlijnen voor het veilig gebruik van eigen apparaten[11] (Bring Your Own Device). Dit omvat het scheiden van persoonlijke en werkgegevens en het volgen van de universiteitsspecifieke beveiligingsprotocollen.
- Neem deel aan beveiligingsbewustzijnstrainingen die door de universiteit worden aangeboden. Dit helpt bij het herkennen van phishing-aanvallen en andere cyberdreigingen.
- Vermijd openbare Wi-Fi en gebruik geen apparatuur van derden.
- Gebruik geen USB-opslagmedia
- Gebruik geen USB devices van anderen, ook geen opladers of USB-poorten in auto’s of vervoer e.d.
- Vermijd het bespreken van vertrouwelijke informatie in openbare ruimtes.
- Als er iets verdachts gebeurt met een device, dan gebruik je het niet meer.
- Schakel Bluetooth (en indien mogelijk ook Wifi) uit.
- Meld incidenten of verdachte situaties waarvan je niet weet hoe daarmee om te gaan, direct aan CERT-UT[12].

[10] Wijzig je wachtwoord indien je een vermoeden hebt van misbruik van je inlogaccount
[11] https://www.utwente.nl/nl/cyber-safety/cybersafety/wetgeving/gebruik-van-eigen-apparatuur-nl.pdf
[12] https://www.utwente.nl/nl/cyber-safety/meld-incidenten/

## MAATREGELEN MIDDEN RISICOPROFIEL

- Neem geen of zo min mogelijk vertrouwelijke gegevens mee, zowel digitaal als op papier.
- Vervoer vertrouwelijke documenten in de handbagage.
- Gebruik altijd versleutelde communicatie en eduVPN-verbindingen.
- Versleutel gevoelige bestanden die je op jouw laptop opslaat.
- Maak altijd gebruik van versleuteling als je gevoelige informatie uitwisselt. Bijvoorbeeld filesender[13].
- Beperk de toegang tot gevoelige gegevens tot alleen diegenen die het nodig hebben voor hun werk. Geef expliciete instructies over het gebruik van de gegevens en maak duidelijk dat het delen buiten de projectcontext niet is toegestaan.
- Pas wachtwoorden aan voor en na de reis.
- Wis belgeschiedenis en verwijder berichten van de telefoon.
- Gebruik een wegwerptelefoon met tijdelijke simkaart.
- Vermijd gebruik van hotelkluizen voor vertrouwelijke informatie. Zie 3.1
- Download geen applicaties tijdens de reis.

## 5.4 MAATREGELEN HOOG RISICOPROFIEL

- Maak minimaal 3 weken voor de reis een afspraak met Servicedesk ICT (LISA) voor instructie en voorbereiding.
- Gebruik sealbags voor vertrouwelijke gegevens en apparaten.
- Gebruik voor buitenlandse reizen speciale apparatuur. Dus lege laptop en smartphone in overleg met Servicedesk ICT (LISA).
- Lever apparatuur altijd in bij de Servicedesk LISA voor analyse, wissen en herinstallatie na de reis.

[13] https://www.surf.nl/diensten/surffilesender

# 6 CONTACTGEGEVENS

| WIE | | |
|---|---|---|
| **CERT-UT** | Computer Emergency Respons Team UT | https://www.utwente.nl/en/cyber-safety/reportincident/<br>+31 53 4891313<br>cert@utwente.nl |
| **Servicedesk ICT (LISA)** | Support Requests | servicedesk-ict@utwente.nl<br>+31 53 4895577 |
| **KST-UT** | Knowledge Safety Team UT | knowledge-safety@utwente.nl |

# 7 REVIEW VAN DIT BELEID

Dit beleid wordt minimaal iedere drie jaar herzien. De volgende herziening vindt plaats medio 2027. Er kunnen reden zijn voor een tussentijdse evaluatie. Als die evaluatie er aanleiding toe geeft zal het beleid eerder worden aangepast.

De CISO van de Universiteit Twente is verantwoordelijk voor dit beleid.

Dit beleid wordt vastgesteld door het CvB van de Universiteit Twente.