Internal memo

Date:	15.3.2024
To:	All
From:	Arne Hagesæther
Subject:	Policy for travelling with IT equipment

Travelling with IT equipment (Laptop, mobile phones)

The political world situation is changing, and we are seeing an increased risk globally with regards to cyber threats. Russia, China, Iran, and North Korea are nation-state cyber actors. Travelling to either of these countries need to be done with care and we should ideally avoid bringing sensitive documents as there is a high risk of being monitored and that data traffic can be listened in to.

Note that general company travel guidelines for bookings, hotels etc are located here: HR – ScaleAQ Intranet

Also please review NSMs travel advice on this page that is regularly updated: NSMs travel guidelines for digital security - Nasjonal sikkerhetsmyndighet (Norwegian)

1. Purpose

This IT Travel Policy outlines guidelines and procedures for employees traveling internationally on behalf of the company. The primary objective is to ensure the security of company data and IT assets while maintaining productivity during travel.

2. Scope

This policy applies to all employees, contractors, and consultants traveling internationally for business purposes on behalf of the company.

3. Responsibilities

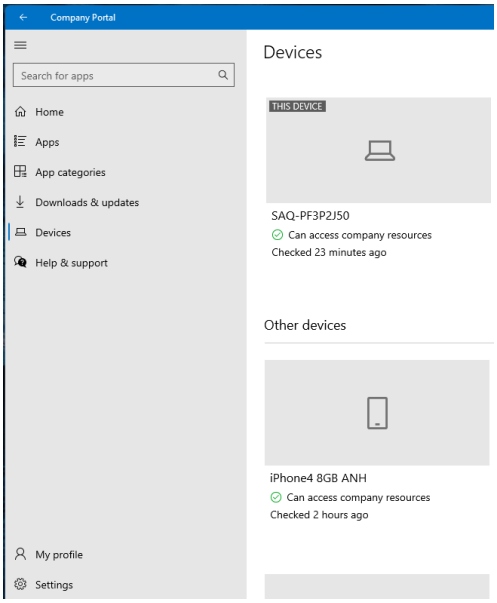
Employees: It is the responsibility of employees to adhere to this policy and exercise caution when using company IT resources during travel.

IT Department: The IT department is responsible for implementing necessary security measures, providing support to travelers, and enforcing compliance with this policy. Contact itsupport@scaleaq.com with regards to any questions related to this document.

4. Pre-Travel Preparations

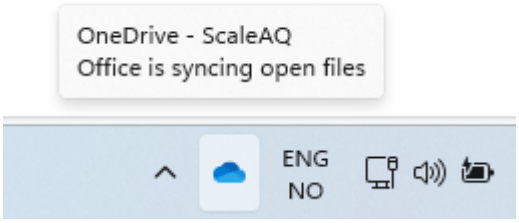
- Travel Authorization: Employees must obtain approval from their respective managers before making any travel arrangements. https://intranet.scaleaq.com/divisjoner/scaleaq/hr/#reiser

- Device Preparation: Employees must ensure that all company-issued devices (laptops, smartphones, tablets) are compliant with the latest security patches, antivirus software, and encryption tools before traveling. A status for this is available in the Company Portal (Firmaportal), click Devices on the right hand side and check for the status “Can access company resources” as on the image below. Click into each device for more information.



- Mobile devices need to be enrolled and managed according to this procedure: Mobile Device Management (MDM) – ScaleAQ Intranet
- Laptops need to be enrolled and managed, review this document on how to confirm: IT-Support.pdf (scaleaq.com)

- Backup Data: Employees must back up all critical data stored on their devices to company-approved cloud storage. ScaleAQ use OneDrive as cloud storage. Ensure you don’t have any sync conflicts and you store critical documents in OneDrive, SharePoint or in the company’s selected software.



- Mobile Data usage: Be careful and monitor data consumption to avoid unnecessary cost, check with your phone provider for available data packages if needed.

  Norwegian users. Ensure you have “Min Unifon” app installed, monitor your data usage and if you need buy suitable data packages this can be done via the “Min Unifon” app or Unifon My page

  Check the cost for data in the country you are travelling to here: Price information abroad - Unifon

- Travelling outside EU. Note that for Seabased, Software and Group using Unifon we have enabled a limit on speed to 40kbit/s prior to purchasing any data package. When arriving in your destination you will get an SMS with price information for calling and data. When you have spent kr500 you will get an SMS warning you prior to accepting to continue, next warning is after you have spent kr16000 and if you accept to continue it will run until kr32000 upon this point data/calls will be blocked.
  Hence this big cost

5. During Travel

Device Handling: Employees must always keep company-issued devices with them during travel and avoid leaving them unattended in public areas.

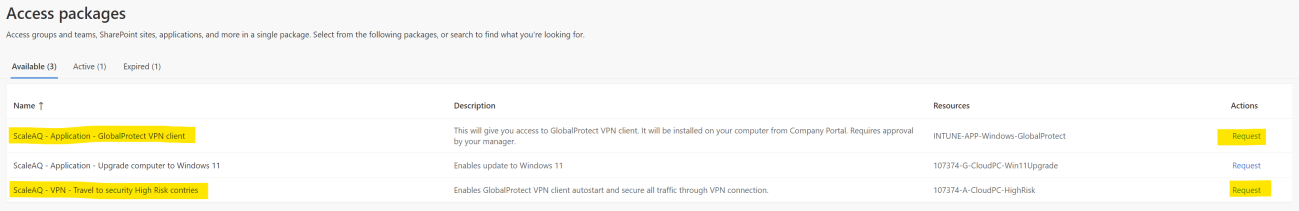
If you are forced by authorities to hand off or give access to mobile device or laptop inform itsupport@scaleaq.com

Public Wi-Fi: Employees should avoid connecting to public Wi-Fi networks whenever possible. Travelling abroad, they must use a virtual private network (VPN) to encrypt their internet connection.

VPN:

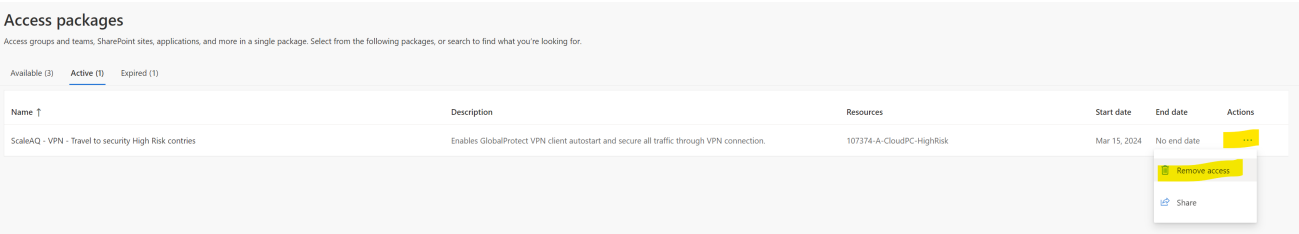
My Access (microsoft.com)

When planning to travel abroad install the “ScaleAQ – Application - GlobalProtect VPN client” and reboot your computer. Note the installation is set to be approved by your manager so provide some time prior to travelling.



Before leaving your home country enable the “ScaleAQ – VPN – Travel to security High Risk countries”

Upon returning home go to active packages and remove access.



Email and Communication: Employees must use company-approved email and communication tools for work-related correspondence. Personal email accounts should not be used for business purposes.

Data Security: Employees should exercise caution when accessing and sharing company data while traveling. Confidential information should be stored securely and not left exposed in public spaces.

Cyber Crime: If you notice your device is compromised, hacked, you are threatened and know 3rd party has unwanted access to your data we have a 27/7 Security Operation Centre available at +4797707000 you can reach out to.

6. Lost or Stolen Devices

In the event of a lost or stolen device, employees must:

- report the incident to Advania Support +4766776577 giving customer number 107374 and
- report to local authorities immediately. (Any insurance case requires you to report it to local authorities and get a police report to be effective https://intranet.scaleaq.com/divisjoner/scaleaq/hr/#forsikringer)

The IT department/Advania Support will initiate remote wiping procedures to erase sensitive data from the lost or stolen device to prevent unauthorized access.

7. Post-Travel Procedures

Upon returning from travel, employees must report any security incidents or breaches to the IT department at itsupport@scaleaq.com

If there has been a known security breach during travel employees must reset the device prior to connecting it to the company network.

8. Compliance and Enforcement

Non-compliance with this policy may result in disciplinary action, including but not limited to suspension of travel privileges, loss of access to company IT resources, or termination of employment.

9. Review and Updates

This IT Travel Policy will be reviewed periodically by the IT department to ensure its effectiveness and relevance. Updates will be communicated to all employees accordingly.

10. Conclusion

By adhering to this IT Travel Policy, employees contribute to the protection of company data and IT assets while traveling internationally on business. Compliance with these guidelines is essential to maintain the security and integrity of our organization's IT infrastructure.