Device security for travel and telework abroad

April 2023 | ITSAP.00.188

Traveling with mobile devices can pose risks to you and your organization. These risks can be amplified if you are teleworking abroad. This publication provides advice and guidance to employees traveling or working abroad with corporate devices. While a list of country-specific risks is not available, this document consolidates information on the risks and mitigation measures you should consider before, during, and after traveling or working abroad with your devices.

You should carefully consider the potential risks of using devices while travelling outside of Canada. Each travel scenario will require an assessment to determine the risk associated with the travel scenario. If a device is issued for travel or for telework agreements abroad, ensure your employees are educated on the policies governing the use of corporately owned devices outside of Canada. Your organization should consider the following when completing a risk assessment for individual travel or foreign telework agreements.

High profile travelers

Senior executives and those working with valuable information are at a higher risk of being targeted by threat actors. The devices of high-profile travellers contain sensitive information and if they are compromised, it could be used for malicious purposes, such as extortion.

Consider assigning “travel devices” instead of corporate or personal devices for high profile travellers or employees attending high profile events. If however, corporate devices are assessed to be an acceptable risk, then the appropriate security controls should be applied, and the traveller should complete awareness training.

For more information on device security while travelling in a high-profile position see, Mobile Device Guidance for High Profile Travellers (ITSAP.00.088).

High profile events

When traveling to high profile events, like global conferences or summits, state events (e.g. state funeral, celebratory function of state officials), or a global event like the Olympic games, a mobile device is required for you to conduct business. Due to the increased attention on the event you attend, implementing additional security measures to protect your device and yourself is recommended.

Employees traveling to high profile events should be issued travel devices that are connected to a segregated enclave and subject to enhanced monitoring.

For more information on device security while travelling for business, see Mobile Devices and Business Travel (ITSAP.00.087).

Short-term stays

When travelling with a device for a short period of time, the security of your device should be paramount. If your organization has issued you a travel device, ensure you know the limitations of the device and your use while abroad. If you received permission to use your corporate device, ensure you follow the device security checklist provided in this publication.

Teleworking abroad

Long-term teleworking outside of Canada can put your organization at risk. The following should be taken into consideration when approving telework agreements abroad:

If you have teleworkers who need to access sensitive information, your organization should ensure your policies indicate the need for “safe areas” within organizationally controlled facilities abroad. Employees would be permitted to access sensitive information in these approved areas only. If this is not feasible, you should use reasonably private locations such as hotel room or your home abroad, instead of public areas or hotel lobbies for less sensitive business.

In unsecured locations, work should be limited to a low sensitivity level and should be conducted on a corporately approved device. Consider the following measures to enhance the security of your telework agreements abroad:

- Ensure employees connect to your organization’s IT environment with a corporately approved device that enforces disk encryption and multi-factor authentication (MFA)
- Connect all approved devices through a secure VPN
- Use secure web mail access, as it offers additional measures over VPN (to isolate and protect your infrastructure)
- Avoid connecting to Wi-Fi network and use your corporately-issued mobile device as a hotspot for Internet access. Local Wi-Fi networks may be unsecure or have lax security controls applied, leaving your device and connected systems and networks vulnerable to cyber threats.
- Protect your hotspot with a passphrase or complex password and have the highest level of encryption supported by your provider
- Establish clear procedures to govern what the employee is allowed to do with corporate computer resources

Communications Security Establishment | Centre de la sécurité des télécommunications

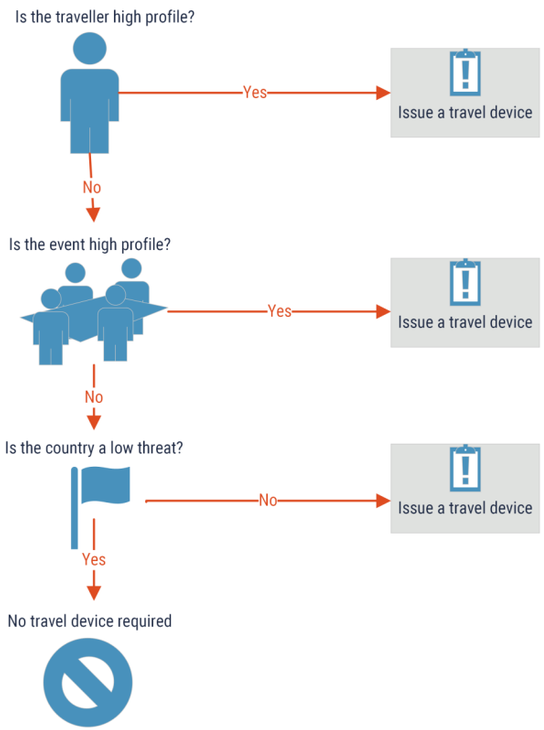
Canada

Risk likelihood considerations and travel devices

Your organization should consider any risks introduced by international travel and telework scenarios and determine your level of tolerance. You should ensure the appropriate measures are implemented to mitigate the risks identified.

Is a travel device needed?

Determining whether to issue a travel device for a specific travel scenario or telework arrangement is contingent on many risk factors and security considerations, primarily based on the traveller, the event, and the destination. Consider the following matrix to help determine whether your employee can travel with their corporate device or whether a device specific for their travel scenario should be issued.



High risk travel

In addition to the profile of the traveller or event, the travel destination must also be considered. Other nation's telecommunication infrastructures may not safeguard your information like those in Canada. When assessing risk and threat levels, your organization should qualify the threat likelihood for travel with devices in accordance with the travel risk levels used by Global Affairs Canada (GAC). They categorize the risk levels of individual countries as:

- Take normal precautions
- Exercise a high degree of caution
- Avoid non-essential travel
- Avoid all travel

While a country may be ranked as a high risk, there could be regions within it that are actually considered to be lower risk. When reviewing the GAC risk levels for your travel scenario assessment, ensure you review the entire country profile to identify the pertinent risks by region. The varying risks levels by region could impact the overall risk assessed for the travel scenario

Your organization should also consider the following items when the travel risk associated to an individual travel scenario is higher on the GAC risk level matrix:

- Prevent your employees from using their regular business or personally owned devices. If they must use a personal device, ensure they turn off Bluetooth, Wi-Fi and location sharing functions.
- Enforce the use of a virtual private network (VPN) to connect to any corporate network or system.
- Ensure your IT department has an inventory of travel devices, and if necessary, restricted travel accounts to limit system and data access while your employee is travelling in a high-risk or high-threat environment.
- Encrypt information on the devices your employee will take while travelling prior to their departure as communications transmitted over public carriers are at risk of being intercepted.
- Assume that hotel Internet connections, photocopiers, or fax machines are monitored and use them for non-sensitive information only.
- Instruct your employee to report any unusual device performance issues or any other associated security concerns to your IT security department.

When assessing your travel scenarios, always consult the Global Affairs Canada (GAC) travel advisory page to get the most recent information on country-specific risk levels, crime trends, and recommended security precautions.

How do threat actors target travellers?

Threat actors are interested in the data your devices possess and the access they might have to your corporate networks and systems. They typically can use commercial eavesdropping devices (e.g. International Mobile Subscriber Identity [IMSI] catchers) to do the following:

- Identify and target mobile devices
- Access the device and track your location
- Use the device's network connections , like Wi-Fi and Bluetooth
- Deliver malicious code to the device
- Activate the microphone or camera on the device
- Intercept communications

Checklist for device protection while traveling or working abroad

- ☐ Update the software, firmware, and operating systems (OS) of corporately-owned devices regularly.
- ☐ Ensure devices and other media are encrypted with the highest level permitted for the device
- ☐ Enable MFA on devices and accounts
- ☐ Install anti-virus , anti-malware, and anti-phishing software on devices
- ☐ Use web browser plug-ins for ad-blocking and malware-blocking
- ☐ Implement access control for all devices that include passphrase or password protection
- ☐ Use device hygiene mechanisms such as domain name system (DNS) filtering
- ☐ Backup your devices prior to departure
- ☐ Minimize the information stored on corporate devices to files required for the travel scenario only
- ☐ Remove stored credentials and passwords for accounts and services that do not need to be accessed while on travel or working abroad
- ☐ Change the passwords for all accounts, especially those that have shared or common access rights
- ☐ Disable features such as GPS, Bluetooth, and Wi-Fi when not needed
- ☐ Turn off automatic connection capabilities so your devices will not connect or pair automatically with unknown devices or unsecure networks
- ☐ Avoid unnecessary application downloads and limit application use on your devices
- ☐ Monitor your device for unusual behavior, such as performance issues, pop-ups, or reduced battery performance
- ☐ Keep track of your devices, including cables, chargers, and peripherals as they can contain embedded micro-controllers to deliver malware

Communications Security Establishment | Centre de la sécurité des télécommunications

Canada