Policy number	Title:	Effective Date:
<your ID format>	GUIDANCE FOR INTERNATIONAL TRAVEL	<your date format>

SUPPORTING DOCUMENTS

- **This is a contents link space for any related documentation**

PURPOSE

The purpose of this document is to offer guidance to travelers on how to protect **<company name>** data and information systems when travelling to, what could be considered, 'high-risk' countries. It should be assumed that, when travelling, your electronic devices may be accessed either physically or electronically, to steal information you have, or inject malware to gain remote access to your devices, and/or infect your organization's network when you return.

SCOPE

Anyone travelling with **<company name>** owned equipment, or anyone planning to access **<company name>** resources while travelling.

The following advice is not intended to be exhaustive but is an attempt to provide a framework of guidance to choose from.

DEVICE SECURITY

- **Consider** using a 'burner' mobile phone or laptop device when travelling to very high-risk locations. Burner devices can be provided by your business <**specify delivery time**>. ***Note:*** *A burner mobile phone would be taken with you instead of your normal mobile phone. It would be only equipped for phone calls and would have no ability to run apps..*
  A burner laptop would have nothing installed other than the ***<company name>*** *sanctioned software. There would be no rights to install any apps or software on either type of device.*
- Only carry essential devices that are free of sensitive data.
- Consider using an Apple iPad or a mobile phone instead of bringing a laptop.
- If you do bring your **<company name>** laptop, ensure all non-relevant sensitive data is removed before travel. Ensure all installed applications are

fully patched and that **<company name>**'s sanctioned security software is enabled and working.
- Ensure your laptop disk is fully encrypted.
- If you take your **<company name>** laptop with you on your travels, ensure important documents are backed up before you travel. It may get lost, or it may be necessary to format and rebuild the laptop on your return.
- Never leave your phone, tablet, or laptop unattended.
- Tr to use biometric authentication where possible.
- You should consider changing your **<company name>** password before you leave.
- You should change your **<company name>** password immediately on return.

UNSECURED NETWORKS

Hostile actors have access to networks, including hotel networks and Wi-Fi. This raises the likelihood of sensitive information (sensitive files, passwords/credentials) being stolen.

- Refrain from using SMS or Bluetooth services.
- If you need to use a computer, where possible, try to use secure remote protocols (e.g RDP) to computers in safe and known locations – for example to an **<company name>** hosted computer.
- Use the **<company name>** provided VPN at all times.
- Never connect **<company name>** equipment to unauthorised third-party VPNs.

DATE ISSUED/DATE REVIEWED

Date Issued:	MM/DD/YYYY
Date Reviewed:	MM/DD/YYYY