**Travel Security for Researchers**

Follow MacEwan's established travel management protocols, established by Health, Safety & Environment.

When travelling, consider these practices, as established by Universities Canada:

- Review your web presence (social media and other profiles) to ensure you are aware of what information about you is available.
- Limit information provided on travel applications and visas and the information provided to border patrol agents to only what is required.
- Exercise caution when interacting with people.
    - Elicitation: you are engaged in what seems like harmless or random conversation, but information about you, your work and your colleagues is subtly being gathered. The people you interact with that are eliciting information may be legitimate researchers, students, impersonators, and people may be employed by governments or groups to appear in everyday roles to gather information about foreigners.
    - Cultivation: a relationship is developed to extract information
    - Sexual entrapment for blackmail: an individual using sex to lead you into a compromising position, such as the recording of an intimate encounter which is then used to blackmail or publicly embarrass the victim
- Do not talk about sensitive parts of your research in public places or to people you have just met. Monitor the progress of associations, particularly new relationships and connections with foreign nationals and refrain from offers of personal companionship while travelling.
- The risk of theft occurs at hotels, conference spaces, in cars, etc. Do not travel with unnecessary electronic or physical files or devices.
- Ensure you keep details of your accommodation private. Avoid using hotel or conference computers or public phones and do not surrender electronic devices at conferences.
- Cyber intrusion can occur with wireless and telecommunication networks, and access to information on your devices can be attained. Any device that can be plugged into your computer's USB drive is a potential threat. Consult with ITS regarding securing devices by starting a chat in-person or online with the MacEwan Help Centre.

- Carefully consider what data you need while travelling. Ideally, it is best to store data on MacEwan's approved cloud storage services such as Microsoft OneDrive and/or Google Drive. If it is necessary to transfer data to a separate external storage device, consider encrypting it and ensure that you keep with you at all times while travelling. Only access cloud data storage services on personal and secure devices.
- If your device has been stolen or lost, you must immediately report the theft to ITS by submitting a Cyber Security concern request. If your device has been left unattended, or if foreign items have been plugged into your device, consider it compromised and consult with ITS for next steps.
- If any of the personal online services that you use (such as your bank, social media, travel websites) support the use of Multi-Factor Authentication (MFA) it is highly recommended that you enable these services.