UNIVERSITY OF SASKATCHEWAN

# ITEM FOR INFORMATION

**Committee Name:** Research, Scholarly and Artistic Work Committee, University Council
**Date:** May 14, 2026
**Presented by:** Eric Lamb, Chair, Research, Scholarly and Artistic Work Committee

**Subject: Device Security and Research Travel Security**

**SUMMARY**

At its March 12, 2026, meeting, RSAW met with Lisa Belhumeur, Senior Research Security Specialist, Research Acceleration and Strategic Initiatives, Jon Coller, Chief Information Security Officer and Karim Panjvani, Research IT Security Coordinator to discuss device security and security best practices for traveling researchers. The committee found the information extremely valuable; therefore, is being brought to Council to broaden awareness.

The presentation described a growing collaboration between the Research Security Office (RSO) and Information and Communications Technology (ICT) to help reduce the risks associated with travel, especially international travel. Travel security brings together national security obligations (such as sanctions and export controls), Canadian research security policies, funding requirements, IT security, and personal safety considerations. When researchers or staff travel for conferences, meetings, or fieldwork, they often carry devices that provide access to sensitive research data, institutional systems, or controlled information. If those devices are lost, inspected, compromised, or intercepted, this can lead to legal, policy, or funding-related issues for both the individual and the university.

To address these risks, the RSO offers tailored travel security briefings that take into account who is travelling, where they are going, and what they will be doing. Particular attention is paid to higher-risk destinations, such as China, Russia, and Iran, though guidance can be provided for any location. These briefings are designed to raise awareness of how foreign intelligence services may target travellers, common recruitment or coercion tactics, detention risks, and behaviours that can increase or reduce personal and institutional risk. The intent is not to alarm travellers, but to equip them with practical information so they can make informed decisions and recognize situations that may warrant caution or follow-up.

ICT's contribution focuses on protecting data and devices while travelling. The core message is to minimize the amount of data taken on trips, as devices used outside institutional control are more exposed to theft, inspection, or compromise. Guidance emphasizes protecting credentials, using secure storage solutions instead of local files, being cautious with public and hotel networks, avoiding public charging stations, and keeping devices physically secure. These practices reduce the potential impact if a device is lost, accessed, or seized and reinforce the shared responsibility for safeguarding institutional systems and information.

Looking ahead, RSO and ICT are working toward a more formal travel security program, currently in the planning stages. A future pilot, targeted for fall 2026, would test an integrated approach that combines travel security briefings with IT guidance. The long-term goal is to make travel security guidance more accessible, practical, and easy for the university community to follow, while strengthening overall protection of people, research, and institutional assets.

For more information or to book a travel consultation contact Lisa Belhumeur: Belhumeur.lisa@usask.ca