INFORMATION SECURITY GUIDELINE

Security Considerations for International Travel with Mobile Devices

Introduction

1. Special considerations may apply when encrypted devices are taken outside Canada. UBC employees should understand these restrictions to avoid the confiscation of their device, or other penalties. The following information is for reference only; all faculty and staff should contact the countries that they are planning to visit to determine what the requirements are in those jurisdictions.
2. This guideline has been issued by the Chief Information Officer to supplement the Encryption Requirements standard. Compliance with this guideline is recommended, but not mandatory. Questions about this guideline may be referred to information.security@ubc.ca.

How to Avoid Problems

3. The best way to avoid issues is to remove any encryption software from the device prior to travelling. Please note that you can only do this if you remove all Confidential information from the device as well. It is much more secure to log in remotely to UBC servers than to carry Confidential information with you. However, if you must have Confidential information saved on your device, then encryption is mandatory under the Encryption Requirements standard. For faculty and staff who need them, the University typically makes “loaner laptops” available for travel purposes but this varies amongst Faculties and Departments.

Canadian Export Controls on Encryption Products

4. Because encryption products can be used for illegal purposes, including terrorist activity, Canada restricts the export of some encryption products to the following countries: Cuba, Iran, North Korea, Sudan, and Syria. Travellers visiting these countries may not have encryption products installed on their computers unless they have a special export license; check with UBC IT Security for more details.

Foreign Import Controls on Encryption Products

5. Some countries ban or severely regulate the import and use of encryption products.
6. Under a set of rules known as the "Wassenaar Arrangement”, travelers may freely enter a participating country with an encrypted device under a "personal use exemption" as long as the traveler does not create, enhance, share, sell or otherwise distribute the encryption technology while visiting. The countries that support the personal use exemption include: Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, New Zealand, Norway, Poland, Portugal, Republic of Korea, Romania, Slovakia, Slovenia, South Africa, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States.
7. The following nations do not recognize a "personal use exemption". Before traveling to these countries with an encrypted device, travelers will need to apply to the specified governmental agency for an import license:
    a. Belarus - a license issued by the Belarus Ministry of Foreign Affairs or the State Center for Information Security of the Security Council is required.
    b. Burma (Myanmar) - a license is required, but licensing regime documentation is unavailable.
    c. China - a permit issued by the Beijing Office of State Encryption Administrative Bureau is required. The laws in China vary from province to province where the customs officers or border guards make their own interpretation of what encryption means.
    d. Hungary - an International Import Certificate is required.
    e. Iran - a license issued by Iran's Supreme Council for Cultural Revolution is required.
    f. Israel - a license from the Director-General of the Ministry of Defense is required. For the applicable laws, policies and forms, see the following website: http://www.mod.gov.il/pages/encryption/preface.asp.

g. Kazakhstan - a license issued by Kazakhstan's Licensing Commission of the Committee of National Security is required.
h. Moldova - a license issued by Moldova's Ministry of National Security is required.
i. Morocco - a license is required.
j. Russia - licenses issued by both the Federal Security Service (Federal'naya Sluzhba Bezopasnosti - "FSB") and the Ministry of Economic Development and Trade are required. License applications should be submitted by an entity officially registered in Russia. This would normally be the company that is seeking to bring an encryption product into Russia.
k. Saudi Arabia - it has been reported that the use of encryption is generally banned, but research has provided inconsistent information.
l. Tunisia - a license issued by Tunisia's National Agency for Electronic Certification (ANCE) is required.
m. Ukraine - a license issued by the Department of Special Telecommunication Systems and Protection of Information of the Security Service of Ukraine (SBU) is required.

8. In addition to import controls, some countries have regulations restricting the use of encryption. The most prominent are France, South Africa, China and Russia. For more information see: Export permits for cryptographic items.
9. Since laws can change at any time, check before travelling to ensure that you have the most up-to-date information. Additional information about international encryption controls can be found at the following websites:
    a. Crypto Law Survey
    b. Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Good and Technologies

Providing Passwords to Law Enforcement Officials

10. In many countries, customs or other law enforcement officials are authorized to require travellers to unlock a device or produce a password. Refusal to comply may result in denial of entry, arrest, or confiscation of the device.
11. If asked by an official to unlock a device or provide a password, UBC employees should advise the official that the device contains confidential University information. If the official persists, the employee may comply with the demand. In such cases, the employee should make reasonable efforts to keep the device in sight at all times, and should change passwords and report such access to UBC Information Security as soon as possible.

Related Documents

Policy 104, Acceptable Use and Security of UBC Electronic Information and Systems

Encryption Requirements standard