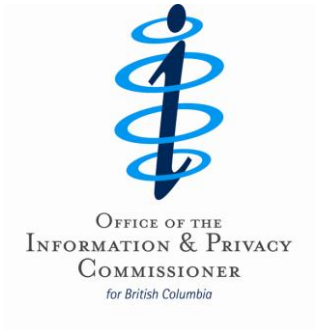

NEWS RELEASE
For Immediate Release
Mar. 29, 2012

UVic failed to protect personal information in privacy breach

VICTORIA—The University of Victoria failed to protect personal information as required by law in a significant privacy breach earlier this year, says a report released today by B.C.'s Information and Privacy Commissioner.

Commissioner Elizabeth Denham launched an investigation when a USB flash drive containing the names, SIN numbers and banking information of nearly 12,000 current and former University employees was stolen in January. The device has not been recovered. Police continue to investigate.

"This is a significant privacy breach affecting thousands of British Columbians. Since our investigation was launched, my office has heard from current and former University employees, who are deeply worried about their exposure to bank fraud, identity theft and other harms.

"What is very unfortunate is that this privacy breach was both foreseeable and preventable. Instead of a simple theft of a mobile device, the incident resulted in enormous costs and stress for those affected and for the University," said Denham.

While the University has established privacy and security policies in recent years, the institution failed to implement reasonable safeguards to protect data stored on the USB drive. Such safeguards are a legal requirement under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

"Encryption is the minimum standard for devices like laptops and USB drives. The University was aware of their obligation to safeguard sensitive personal information using a range of protective measures including readily-available and widely-used encryption solutions." Denham said.

The investigation also assessed the University's response to the privacy breach, and found that the University had satisfied its legal obligations under B.C. privacy law.

"The University took immediate steps to contain the breach following the discovery of the loss of employees' personal information. They quickly recognized the significant risk to employees, notified affected individuals and are developing short and long-term strategies to prevent this from happening again," said Denham.

The commissioner made ten findings and five recommendations. Three of the recommendations are aimed at improving the University's privacy management program.

-30-

Summary of recommendations

1. The University of Victoria should formally review their privacy and security policies at a minimum of every three years.

2. The University should re-assess the physical security of the Financial Services area to determine whether it is necessary to alarm the entire building, and to assess other buildings on campus where personal information is stored.

3. The University should develop a comprehensive policy, procedure, training and technical solution to ensure that personal information stored on laptops and other mobile security devices is protected as required by Section 30 of FIPPA. This policy and training program should include issues of data limitation, encryption, appropriate password maintenance, physical security, wireless security and proper disposal.

4. The University should develop a policy that requires the privacy manager to conduct risk assessments of personal information data banks on an annual basis and report to the University President on the result of these assessments.

5. The University should provide a copy of the report of the external consultant to my office for review and comment prior to its finalization.

Media Contact:

Cara McGregor
Manager, Communications and Public Education
Office of the Information and Privacy Commissioner for B.C.
250 217-5535