University of Victoria

Terms of Reference for an External Review of January 2012 Theft of Employee Personal Information at the University of Victoria

The University of Victoria is intent on avoiding any repetition of the recent theft of employee personal information that alarmed the university community and the general public.

To this end, it is commissioning a comprehensive external review by a recognized international expert. The review will be conducted by Dr. David Flaherty, a specialist and consultant in privacy and information policy issues who served as Information and Privacy Commissioner of British Columbia from 1993 to 1999. Dr. Flaherty will bring the most up-to-date knowledge and expertise to bear on the issues and will provide a report to the President and the Board of Governors with recommendations on the physical security and information security of sensitive personal information in the custody or control of the University of Victoria. His work will include:

- conducting needed interviews and site visits and collecting information as necessary;
- reviewing findings and recommendations arising from the operational response (including communication) that took place and from the internal assessment that is being carried out, as well as actions taken by the university in response to those.

The external review will address whether the university has identified the lessons to be learned from the January 2012 breach and developed appropriate plans, or implemented appropriate measures, to protect sensitive personal information across the university. Questions to be addressed will include:

- Is the university making all reasonable efforts to identify, review and protect sensitive personal information resources in the custody or control of the university?
- Are there storage systems containing sensitive personal information at the University of Victoria that are not adequately protected?
- Are the university's privacy, records management, physical security and information security policies, procedures and practices adequate to meet needs, standards, and statutory requirements in 2012?

The external review is expected to be completed within four months. The report will be public, although some associated material may of necessity remain confidential for reasons of security, personal privacy or other grounds permitted under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

At Dr. Flaherty's recommendation, the university is carrying out an internal assessment as part of the process. The terms of reference for the assessment have been approved by the external reviewer. The internal assessment will be led by Professor Jamie Cassels of the Faculty of Law. Professor Cassels will seek and receive input from members of the university community and will be able to call upon individuals within the institution with intimate knowledge of existing policies, procedures, and practices related to this matter. Operating under the guidance of the external reviewer, the internal assessment will:

1. identify and assess the steps leading up to the incident, commencing with the decision to create the stolen data storage device.

2. analyse the business processes related to the incident (e.g., data management, business continuity planning) and their oversight and identify what changes should be made in the future related to decision-making processes, accountability, and implementation;

3. review information security, physical security, privacy and records management policies, procedures and practices related to the incident:
    - were the relevant policies and procedures followed in this instance?
    - do the policies and procedures appear to be adequate?
    - what changes are recommended?

4. ascertain and review:
    - the steps taken since the incident to identify storage systems containing sensitive personal information at the university and to mitigate any significant risks;
    - the university's plans for: identifying other sensitive personal information resources on campus; assessing the levels of risk associated with them; and reviewing their collection, use, storage and disposition;

5. seek input and receive questions from the campus community regarding the treatment of sensitive personal information at the university and recommend how the university should address the issues raised;

6. determine whether the university has appropriate plans for reviewing information security, physical security, privacy and records management policies and procedures on an ongoing basis and assessing and achieving compliance;

7. identify any systemic questions or issues that might best be addressed by the external reviewer;

8. report findings and recommendations to the external reviewer and the university.

The findings from the internal assessment are expected to be ready within three months. The internal assessor's report and the administration's response to it will be public, although some associated material may of necessity remain confidential for reasons of security, personal privacy or other grounds permitted under FIPPA.

The University of Victoria is also cooperating fully with an independent investigation initiated by the Office of the Information Privacy Commissioner of British Columbia (OIPC). Information from the external review and the internal assessment pertinent to the OIPC's investigation will be shared with that office as it becomes available.

Note: Sensitive personal information is personal information that is confidential or highly confidential under UVic's University Information Security Classification Procedures. The University is aware that FIPPA requires it to have reasonable security for all personal information in its custody or control.

University community members who wish to provide input into the review process may do so through Prof. Cassels, by e-mail at privacyreview@uvic.ca .