OFFICE OF THE
Auditor General
of British Columbia

NEWS RELEASE

For Immediate Release

August 13, 2019

Key controls in place to prevent unauthorized access to government systems

VICTORIA – The Office of the Auditor General of British Columbia has released a new report, *The B.C. Government's Internal Directory Account Management.*

Every government employee and contractor has a user name and password to access government systems, and government's internal directory system (IDIR) authenticates each user's identity to ensure it is legitimate. To provide services for people in British Columbia, government collects and stores a lot of sensitive and personal information. Therefore, only government employees and contractors who need access to government systems containing sensitive information should have access.

"The IDIR service is the first defense against unauthorized access to government resources," said Carol Bellringer, auditor general. "All it takes is one poorly managed user account to compromise government systems."

The office audited five ministries and found that some of them were not consistently following the Office of the Chief Information Officer's (OCIO) established key controls to restrict unauthorized access. It is important to note that the office did not look for inappropriate use of accounts or security breaches that could result from improper accounts.

The office also found a lack of understanding regarding the role of the OCIO versus individual government organizations as to the responsibility for maintaining the central records of accounts. The OCIO has overall responsibility for managing the internal directory service, and each ministry and government organization manages its staffs' IDIR accounts. "The OCIO needs to remind ministries of their responsibilities as defined in the OCIO's information security standards," Bellringer said.

Some government employees have significant access to and abilities within government systems. For example, a system administrator often has the ability to create or alter accounts for their organization's users. The office found that the activities of these employees were not reviewed consistently to ensure appropriate use.

Finally, employee information and account information are stored in two separate databases. The OCIO has responsibility for the IDIR system, but the Public Service Agency (PSA) holds and maintains the list of current government employees. The office recommends that the OCIO and the PSA compare the two lists to ensure legitimacy. A strong coordination and commitment to key controls and management of IDIR user accounts between the OCIO and across ministries is fundamental to controlling access.

OFFICE OF THE
Auditor General
of British Columbia

The full report is available on the Office of the Auditor General website: www.bcauditor.com.

Bellringer will answer questions pertaining to the report via a news conference only.

News conference date: Tuesday, Aug. 13, 2019

Time: 11:30 a.m. (Pacific time)

Dial-in information:
From Vancouver: 604 681-0260
From elsewhere in Canada and the U.S.: 1 877 353-9184
Participant pass code: 44848#

During question-and-answer period:
To ask a question: press 01
To exit the question queue: press #

About the Office of the Auditor General of British Columbia
The auditor general is a non-partisan, independent officer of the legislature who reports directly to the legislative assembly. The *Auditor General Act* empowers the auditor general and staff to conduct audits, report findings and make recommendations.

Contact us:
For general questions,
call Emily Griffiths
Office of the Auditor General of British Columbia
250-419-6132

www.bcauditor.com

Subscribe to receive report e-notifications at www.bcauditor.com/reach/subscribe