Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F16-01

Ministry of Education

Elizabeth Denham
Information and Privacy Commissioner for B.C.

January 28, 2016

CanLII Cite: 2016 BCIPC No. 5
Quicklaw Cite: [2016] B.C.I.P.C.D. No. 5

TABLE OF CONTENTS

PAGE

COMMISSIONER'S MESSAGE 3

EXECUTIVE SUMMARY 4

1.0 INTRODUCTION AND PURPOSE OF REPORT 6

2.0 BACKGROUND 8

3.0 ISSUES 11

4.0 REASONABLE SAFEGUARDS 11

5.0 RESPONSE TO THE PRIVACY BREACH 21

6.0 PREVENTION STRATEGIES 27

7.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS 28

8.0 CONCLUSIONS 30

9.0 ACKNOWLEDGEMENTS 31

APPENDIX A: CITED POLICIES AND DIRECTIVE 32

COMMISSIONER'S MESSAGE

This report details the circumstances surrounding the loss of a portable hard drive by the Ministry of Education containing the personal information of 3.4 million BC and Yukon students and teachers.

As Commissioner, I have long argued that the responsibility of public servants to safeguard personal information assets is directly comparable to their responsibility to safeguard financial assets.

Fortunately, the Government of British Columbia has a very long tradition of strong financial management, which includes specialized training and record keeping as well as a robust audit function, so the probability of a loss, for example, of $3.4 million is highly unlikely.

Information assets, particularly personal information of citizens, deserve the same respect, rigour and control. While government has rules and policies in place to protect personal information, there is not the same tradition of adhering to these rules and policies and safeguarding personal information.

Regrettably, this report documents evidence that a number of policies were not followed. Unsuccessful staff training and the failure to monitor compliance, such as through a privacy audit program, directly contributed to this significant breach.

If this was actually a situation involving a cash loss of $3.4 million, I believe the government would take rapid, dramatic and decisive action to deal with the situation, including increasing the training of staff and possibly improvements in many aspects of financial management such as record keeping and auditing.

I believe that only when Ministries view personal information assets with the same attitude and care that they view financial assets entrusted to them will British Columbians' trust be earned.

I hope that this report assists with the fundamental attitude change I believe is required. Personal information has great value – its loss has a real and lasting negative impact on British Columbians.

Elizabeth Denham
Information and Privacy Commissioner for British Columbia

EXECUTIVE SUMMARY

On September 18, 2015, government notified the Office of the Information and Privacy Commissioner ("OIPC") that the Ministry of Education ("Ministry") was unable to locate a hard drive containing the personal information of 3.4 million BC and Yukon students and BC teachers.

For most of the students, the information consisted of name, gender, date of birth and Personal Educational Number ("PEN"). For a subset of students, it also included address, type of schooling and grade information. The data also disclosed whether students were part of any of the following groups: cancer survivors; children in care; special needs students; children who withdrew from school and post-secondary students receiving financial assistance.

In 2011, the Ministry had transferred the information from the corporate servers to two portable hard drives: one to be used by Ministry staff and the other to be stored offsite as a backup. There was a record that one of the drives was stored at a warehouse leased by the Ministry for the storage of exams and curriculum materials, but no one could verify whether it had ever arrived at the warehouse.

On September 21, 2015, this office initiated an investigation under s. 42(1)(a) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") to determine whether the Ministry had met its obligations under s. 30 of FIPPA to protect personal information in its custody. The investigation examined whether it had adequate security in place to protect the personal information and whether it met s. 30 requirements in responding to the breach.

The investigation found that the Ministry failed to provide adequate security to prevent unauthorized access, use or disclosure. While there were sound privacy and security policies and directives in place of which Ministry employees were aware, several employees contravened a series of them. The transfer of the data from the Ministry server to the mobile hard drives contravened corporate policy and a recent directive stemming from another high profile privacy breach. The Ministry compounded this contravention by failing to encrypt the information, as corporate information security policies required. This contravention made the information accessible to anyone in possession of the hard drive.

The Ministry also failed to record the existence of these hard drives in an inventory of information assets, as required under corporate policy, or in a directory of Personal Information Banks as required under s. 69 of FIPPA. This contravention made it difficult for the Ministry to keep track of the hard drive. Finally, it failed to store the backup hard drive in a government approved records facility, as required by corporate records management policy. These facilities have the infrastructure to keep records secure and to be able to locate them easily.

On the issue of its response to the breach, the Ministry met its obligations under s. 30 of FIPPA. The Ministry conducted a series of comprehensive searches for the backup hard drive. Its analysis of the risks to affected individuals was appropriate. In the circumstances, it was reasonable to employ indirect notification of all individuals through a public media release and direct notification targeted at more vulnerable groups, where the Ministry had reliable contact information. Finally, the preventative measures it adopted by returning the data from the **office-use** hard drive to the server; developing an inventory of all mobile storage devices; and implementing a privacy management policy were reasonable and appropriate.

The failure of the employees involved in the creation of the hard drives to follow clear privacy and information security policies indicated that the training the employees received was not effective. It illustrated the need for better training, executive leadership and compliance monitoring.

The report includes a series of recommendations to strengthen the security and privacy of personal information.

1.0 INTRODUCTION AND PURPOSE OF REPORT

1.1 INTRODUCTION

On September 18, 2015, government officials notified my office that the Ministry of Education ("Ministry") was unable to locate a portable hard drive containing a large volume of personal information.[1] The Ministry believed that the unencrypted hard drive had gone missing from a locked cage, located in a warehouse leased by the Ministry, where the hard drive was supposedly last seen around May of 2011.

The purpose of storing information on this hard drive was to provide a backup for the purpose of disaster recovery of data and research reports that were being stored on another portable hard drive actively used in Ministry offices.

The Ministry was able to locate the office-use hard drive, from which it determined that the backup hard drive contained the personal information of approximately 3.4 million British Columbia students and teachers and Yukon students collected between 1986 and 2009.

The Ministry is not able to determine when the backup hard drive went missing. To date, the drive has not been recovered.

The OIPC launched an investigation into this matter under s. 42(1)(a) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

The purpose of this investigation is to determine if:

- the Ministry had reasonable safeguards in place to protect the personal information on the backup hard drive;
- it took appropriate action to contain the breach; and
- it took appropriate steps to mitigate any potential harm to individuals affected by the breach.

The report makes recommendations for the purpose of reducing the risk of this type of breach from occurring and ensuring the Ministry meets the requirements of FIPPA to provide adequate security for all personal information in its custody or under its control.

[1] For a description of the circumstances of this discovery see below p. 10.

1.2 APPLICATION OF FIPPA TO THE MINISTRY OF EDUCATION

A public body is defined in FIPPA as "…a ministry of the government of British Columbia". The Ministry of Education is therefore a "public body" and is subject to the provisions set out in FIPPA.

The Commissioner has a statutory mandate to monitor compliance of public bodies with FIPPA to ensure the purposes of the legislation are achieved. The purposes, as stated in s. (2)(1) of FIPPA, are to make public bodies more accountable to the public and to protect personal privacy by, among other things, preventing the unauthorized disclosure of personal information by public bodies.

"Personal information" is defined in FIPPA as recorded information about an identifiable individual, other than contact information. Examples of the personal information compromised in this incident include: names, addresses, dates of birth, gender, grades, schools, Personal Education Numbers ("PEN"), graduation status, financial aid data, type of school (including youth in custody), and select student characteristics (such as special needs, language at home, aboriginality and residency). A smaller number of records included more sensitive personal information (such as teacher retirement plans, education outcomes for cancer survivors, and health and behaviour issues of children in care).

1.3 INVESTIGATIVE PROCESS

Upon notification of this data breach, the OIPC initiated an investigation to examine the Ministry's general security safeguards in place prior to the breach and the Ministry's response to the data loss. The OIPC determined that this action was necessary due to the sensitivity of the information, the numbers of individuals affected by this breach, and the fact that most of the individuals affected were children or youth.

The OIPC interviewed past and present Ministry employees who were thought to have knowledge of the backup hard drive's creation, the storage site and the movement of this hard drive. The investigators interviewed 16 individuals between October 15, 2015 and December, 2015. These interviews explored the following issues:

- decision to place personal information on mobile drives;
- data protection protocols;
- storage considerations;
- timelines; and
- search for the backup hard drive.

Documents and Policies

The OIPC reviewed the following documentation:

- BC Government Core Policy and Procedures manual ("CPPM") and the Information Security Policy ("ISP");
- information about the notification of affected individuals;
- Ministry communications; and
- other relevant documents the Ministry provided.

Privacy Safeguards

This investigation examined whether the Ministry had in place a privacy management program that would ensure it had adequate safeguards and whether the safeguards were effective.

Forensic Analysis

The OIPC contracted a forensic data consultant to analyze and verify the contents of the office-use hard drive.

One of the biggest challenges with this file is the lack of documentation surrounding the use and storage of the backup hard drive. The majority of the employees who worked in the relevant program area had either moved on to other positions, retired or could not recall the backup hard drive. The source of the information collected during the investigation was the recollection of employees who were present when the drives were created. Owing to the passage of time, the testimony was, understandably, often vague, incomplete or inconsistent.

2.0 BACKGROUND

In 2010, the Education Systems Information and Reporting Unit[2] ("Information Department") was responsible for analyzing education data and producing ad hoc and public reports related to student performance and the performance of the education system in general. The Information Department produced the reports at the request of the Ministry, Boards of Education and others interested in educational research. Examples of Information Department research reports include: student completion rates, student performance, grade progression or District student enrolment.[3]

[2] The Education Systems Information and Reporting Unit is now known as the Analysis and Reporting Unit.

[3] In addition to the project work, the Information Department is also responsible for managing research agreements with outside educational researchers. This includes, but is not limited to, university instructors and students who conduct research on various educational issues. Outside

The Information Department used the Education Data Warehouse, which contains the personal information of all students in the K-12 sector, as a source of data. It wrote program scripts to extract the necessary raw data from the Education Data Warehouse. It saved the raw data, the tools used to extract and analyze the data and with the final reports in a project folder. The Information Department disclosed reports on the results of its analysis. These reports normally contained aggregate data, but there are some cases where the Information Department provided personally identifiable data required to respond to a query from a Board of Education.

The Information Department retains the data extracts for the purpose of responding to potential questions related to its findings. In some cases, a Board of Education will ask the Information Department to update a previous report. The Information Department uses the stored program scripts to obtain current data. It uses the stored analytical tools to replicate the analysis completed for the original project. This ensures consistent results in response to follow up requests.

The Information Department completes approximately 600 project reports per year. Each project folder is saved in a master folder, which is labeled by the year in which the project was ordered.

The project folders stored on the hard drive contained personal information of approximately 3.4 million BC and Yukon students and BC teachers. The projects contained personal information of varying levels of sensitivity. More specifically, the types of personal information found in the project files included names, addresses, dates of birth, gender, grades, schools, PENs, graduation status, financial aid data, type of school including in custody, and select student characteristics (*e.g.,* ESL, special needs, language at home, aboriginality, and residency). A smaller number of records included more sensitive personal information (teacher retirement plans, education outcomes for student cancer survivors, health and behaviour issues and children in care).

The Information Department project files had consumed a substantial volume of space on a government Shared Service BC ("SSBC") server.[4] The cost to store Information Department data was estimated to be approximately $14,000 per year.[5] In 2010, the Knowledge Management Division decided to reduce the volume of all data stored on the SSBC's shared server to decrease electronic storage costs.[6] The Information Department believed that, because of this initiative, recommending to the Ministry executive to retain the data on the server

researchers use data from several sources. From our review, it appears that there were only a few project folders relating to outside researchers that contained any Ministry data. Research agreements and corresponding data are saved in the same manner described above.

[4] Email string dated May 26, 2010 to June 6, 2010.

[5] OCIO obtained cost from SSBC.

[6] Email string dated May 26, 2010 to June 6, 2010. Interview December 2015.

was not a viable option. Therefore, it was necessary to develop an alternative storage solution.

In June of 2010, the Information Department unit decided to transfer the project data to mobile hard drives. It purchased two mobile hard drives and downloaded the data to both in March 2011.[7] The office-use hard drive was not encrypted and, as discussed later in this report, it is unlikely the backup hard drive was encrypted.

The office-use hard drive remained with the Information Department for access and updating of project files. The Information Department decided to place the backup hard drive at a government offsite location. An employee entered a note in the Total Records and Information Management ("TRIM")[8] system on May 19, 2011 indicating that the office-use hard drive was placed in a file cabinet located in the Information Department.

The same TRIM report indicates that someone transported the backup hard drive to the warehouse in Central Saanich for secure storage in late May 2011.[9] It notes that they placed the hard drive in a filing cabinet drawer. The filing cabinet was secured in a locked cage where the Ministry stored General Education Development ("GED") exams. One individual confirmed transporting the drive to the warehouse and locking it in the GED cage. However, none of the warehouse employees could remember the hard drive being placed in the warehouse. The warehouse has no record of receiving the backup hard drive. Nor are there any records indicating that this hard drive was ever moved.

In July 2015,[10] an employee in the Information Department suggested the unit purchase another mobile hard drive to back up additional project files. The Information Department re-examined the use of mobile hard drives to back up project data. Staff realized the risk associated with maintaining project data on these drives. It explored transferring the files located on the office-use hard drive back onto the SSBC server and destroying the drive. After consulting with the Ministry Chief Information Officer ("MCIO") the Information Department obtained approval to transfer the data from the office-use hard drive to the SSBC server.

During the course of these discussions, one of the Information Department employees recalled that there might have been a second backup drive and advised management about it. An employee went to the warehouse to retrieve the backup hard drive from the locked cage and could not locate it. The Ministry

[7] Invoice dated June 24, 2010.

[8] TRIM is an integrated Enterprise Document and Records Management System. The government of British Columbia selected TRIM Context™ as the standard information management software program to be used across government. www.gov.bc.ca/citz/iao/records_mgmt/guides/TRIM/Interactive_modules/doc_email/index.html.

[9] Email dated October 6, 2015, provided by the OCIO. Email contains the TRIM report.

[10] Ministry timeline reports and emails.

conducted a series of comprehensive but unsuccessful searches throughout the warehouse, Ministry offices and other sites.[11]

3.0 ISSUES

The issues in this investigation are:

1. Did the Ministry have reasonable security safeguards in place to protect personal information from unauthorized access, use or disclosure, as required under s. 30 of FIPPA?

2. Did the Ministry take reasonable steps in response to the privacy breach as required by s. 30 of FIPPA?

4.0 REASONABLE SAFEGUARDS

Issue 1: Did the Ministry have reasonable security safeguards in place to protect the personal information from unauthorized access, use or disclosure, as required under s. 30 of FIPPA?

Section 30 of FIPPA requires public bodies to make reasonable security arrangements to protect personal information in their custody or under their control. Section 30 states:

> **Protection of personal information**
>
> 30 A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

In the past five years the OIPC has investigated or reviewed over 500 privacy breaches, many of which involved the loss or theft of portable storage devices. We have published numerous investigation reports and two recent audit and compliance examinations that have considered the meaning of s. 30 of FIPPA. In the most recent investigation report examining a breach within the Ministry of Health, I summarized the meaning of “reasonable security arrangements” as follows:[12]

[11] For a more detailed description of the search, see below p. 20.
[12] Investigation Report F13-02, [2013] B.C.I.P.C.D. No. 14.

> The reasonableness standard in s. 30 is measured on an objective basis and, while it does not require perfection, depending on the situation, it may signify a high level of rigor. To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards.
>
> The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, the estimated costs of security, the relationship between the public body and the affected individuals and how valuable the information might be for someone intending to misuse it.

FIPPA authorizes government ministries to collect personal information, including sensitive personal information of children and youth, for the purposes of managing their programs and activities. The portable hard drives at issue contain a very large volume of personal information about students, including information about students who had survived cancer, students who were wards of the province and students who had behavioural issues. Given the sensitivity of the personal information, strong safeguards were warranted. Throughout the course of the investigation, we identified a number of weaknesses in the safeguards the Ministry had in place.

4.1 GENERAL SECURITY ARRANGEMENTS

The Ministry was aware of its privacy obligations under FIPPA. The Office of the Chief Information Officer ("OCIO") provided relevant policies surrounding the information technology procurement and the protection of personal information, including a set of guidelines on how to inventory and secure personal information and devices used to store personal information.

The CPPM and the ISP[13] provide direction on the procurement of information technology. They outline limitations with the use of mobile storage devices. They provide guidance on the authorization, use, management and security of personal information stored on mobile data storage devices.

Chapter 6 of the CPPM requires that "Prior to initiating procurement of all IM/IT-related products or services, ministries must discuss their IT requirements with Procurement Services Branch, SSBC and their IM requirements with the OCIO, which will determine whether a corporate solution will be implemented for the requirement."(6.3.5)

These policies are reasonable and adequate to achieve the objectives of providing adequate security for personal information.

[13] BC Government Core Policy and Procedure Manual (CCPM) and the Information Security Policy (ISP).

When the Information Department decided to purchase the portable hard drives, the Ministry had in place a Ministry CIO responsible for ensuring the Ministry was in compliance with government policy and procedures.

From the interviews and available documentation, it appears that there was a discussion between a member of the Ministry's technical support services and SSBC prior to the purchase of the two hard drives. However, none of the witnesses could recall who was involved or the details of the discussion. One of the witnesses from the Ministry's technical support services stated that they believed based on the documentation that a conversation took place with SSBC regarding security considerations surrounding use of the drives and that SSBC agreed with the plan to purchase them.[14] There is no other evidence to corroborate this conclusion.

There is no evidence that anyone spoke to the OCIO about the suitability of hard drives as an alternative solution to their data storage problem, as required by the CPPM 6.3.5. Therefore, while the policies are sound, the employees did not follow them.

RECOMMENDATION 1:

Ministry staff should be reminded that they must store personal information securely. Complying with the requirement to consult with their MCIO on relevant policy and procedures before making decisions regarding the secure storage of personal information and with CPPM 6.3.5 when purchasing portable storage devices will assist in meeting the Ministry's statutory obligation under FIPPA.

4.2 PERSONAL INFORMATION INVENTORY

The CPPM contains a number of policies that require ministries to classify, inventory and identify an owner of information and technology assets. The owner of the assets is responsible for implementing and maintaining proper safeguards to protect the asset.

Ministries must implement safeguards commensurate with identified risks and security requirements. They must routinely review the security of its information systems (CPPM 12.3.6). Ministries must also maintain and update an inventory of Personal Information Banks, which includes any collection of personal information that can be searched by name or any other unique identifier (CPPM 12.3.3).

[14] Ibid.

In Investigation Report F13-02, I recognized that personal information inventories are essential for the purpose of protecting privacy. I stated:

> In order for a public body to provide adequate security for personal information in its databases, the public body must have a clear idea of where data is collected and stored. A thorough personal information inventory is a fundamental, critically important aspect of privacy compliance. … It would be beneficial for the Ministry to develop an inventory of personal information databases and data flows, with the objective of creating a regularly updated repository for the Ministry. There would be further benefits in periodically reviewing this inventory to identify those dataset extracts and other sensitive information assets that can be archived or deleted.

The two hard drives did not appear in the directory of Personal Information Banks of the Ministry as CPPM 12.3.3 requires. Nor were they included in an inventory of information assets as CPPM 12.3.6 requires. The only documentation of the existence of the backup hard drive was in a TRIM record. Again, the policies were sound, but employees did not follow them.

It is not certain that, even if the Ministry had documented the two hard drives as the policies required, it would have ensured that the backup hard drive could be located. Nevertheless, accurate documentation might have assisted in the search. It also might have alerted someone to the existence of the drive at an earlier stage. It was only when the Ministry was reviewing the storage of project files on the SSBC servers in July 2015 that some employees remembered the existence of the backup portable hard drive.

RECOMMENDATION 2:

The Ministry should comply with the requirement in s. 69 of FIPPA to maintain an accurate inventory of personal information assets in the directory of Personal Information Banks, including all personal information stored on portable storage devices.

4.3 STORAGE POLICIES

The CPPM requires ministries to account for, protect and safeguard equipment from unauthorized access.[15] In 2006, in response to a privacy breach that resulted from the sale of computer tapes that included personal information, the OCIO issued a directive (44692) that related to portable storage devices:

[15] CPPM, 12.3.3 and 12.3.6.

> Information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then deleted from the portable storage device. Government information should be stored on the government network whenever possible to ensure the protection and long term availability of the information.

The decision to transfer the project files from the SSBC servers to portable hard drives contradicted this directive.[16] This clear contravention of a sound policy was the root cause of the privacy breach. The fact that there was a financial imperative to reduce information stored on the server does not justify the contravention of this policy.

Ministries may only store records at approved records centres.[17] Storage sites must contain a level of security proportionate to the sensitivity of the information being stored at the facility, and maintain a detailed inventory of the records stored and their location within the facilities.

The warehouse in question is not a government approved records storage facility. That the building is locked and alarmed, and has never been broken into, does not compensate for the fact that it is not an approved records storage facility and does not have the capability to manage records securely. Storing the drive at that location was a contravention of a fundamental records management policy.

The TRIM entry on May 19, 2011, indicates that the backup hard drive was in the locked GED cage at the warehouse. There is no record at the warehouse of the backup hard drive being received into the custody of the warehouse and none of the warehouse employees even remember the hard drive. Based on the lack of documentation and the recollection of employees, it is clear there were no reasonable inventory controls in place to account for, protect or safeguard the backup hard drive. Without inventory controls it is not possible to corroborate testimony that the hard drive was, in fact, taken to and stored at the warehouse.

RECOMMENDATION 3:

To assist with meeting the statutory requirement to store personal information securely, the Ministry should comply with CPPM policy and the OCIO directive 44692 and transfer all personal information from portable storage devices on to the government network as soon as practicable and delete the personal information from the devices.

[16] See also ISP 6.7.1.

[17] CPPM 12.3.3, Part III: Managing Information: Policy.

RECOMMENDATION 4:

To assist with meeting the statutory requirement to store personal information securely, the Ministry should comply with the requirement that when securing mobile devices off-site, they store them in a government approved storage facility, which would document the handling of the device.

4.4 ENCRYPTION OF PERSONAL INFORMATION ON PORTABLE DEVICES

Information Security Policy 7.3.2 requires that information owners and information custodians must prevent unauthorized access by "Enabling password protection on mobile devices including portable storage devices". ISP 7.7.1 requires that sensitive personal information stored on mobile devices placed at off-site locations must be encrypted to protect the information from unauthorized access.

Without being able to examine the backup hard drive, it is not possible to confirm whether the information was encrypted. The office-use hard drive was capable of encryption, but was not encrypted. One witness stated that they were aware that SSBC required sensitive personal information to be encrypted but this was not SSBC's general practice at the time. Since the data was intended to be stored at what they felt was a secure off-site location, they were not concerned whether the backup hard drive was encrypted.

One witness thought the backup hard drive was encrypted because that was best practice. Another mentioned that encryption was considered but there were concerns about password retention. Employees were not allowed to write down passwords, and some feared that they might forget their passwords and, therefore, would lose access to the data.

In Investigation Report F12-02, I made it clear that encryption was the best practice for storing personal information on mobile storage devices:

> Given the amount and sensitive nature of personal information contained on the University mobile storage device, coupled with the ease of encrypting the information, there is simply no rationale for failing to encrypt this information. Without doubt, encryption is the standard when storing personal information on a laptop or any mobile storage device. The use of encryption must be combined with a strong encryption key.

Encryption in this case would have been a simple and effective method to ensure the security of the personal information on the backup hard drive.

RECOMMENDATION 5:

To assist with meeting the statutory requirement to store personal information securely, the Ministry should ensure that it complies with ISP and CPPM policies regarding encryption. If it stores personal information on mobile data storage devices, it must encrypt those devices.

4.5 RETENTION

The Information Department currently retains the data sets from research projects indefinitely. The Information Department states that it needs to keep this data to reduce the time required to respond to questions or replicate results for future updates. The Information Department has also raised concerns that, because the information in the Data Warehouse may change over time, future data extractions may result in minor differences that would affect the consistency of the reports. Another concern was that extracted data sometimes requires correction. If the Information Department did not retain the corrected data, they would have to replicate the corrections for future reports.

The information technology contractor who analyzed the office-use drive reported that project folders were accessed 140 times over the four year period. On many of these occasions, it was merely updating research agreements, which did not require access to any data. Therefore, on average, the Information Department was only required to access the data fewer than 30 times per year.

While I understand the utility of retaining the data for a limited period of time for operational purposes, these concerns do not justify the risks posed by keeping the project data indefinitely. I am not convinced that the Information Department needs to keep these raw data extracts (which contain the personal information of identifiable students) in the project folder in perpetuity. Clearly, the risk associated with retaining this data indefinitely is not justified by the few times the data is accessed. Moreover, the Information Department already retains the original program scripts used to extract the data from the Data Warehouse, which could be used to replicate the original data sets. While admittedly this would be more time consuming, it would reduce the associated privacy and data security risks.

As with all government records, there should be a legislatively approved schedule to govern the retention of these records. The Legislature approved the Ministry of Education Operational Records Classification System (“ORCS”) in

1989. Unfortunately, the ORCS does not have a schedule that clearly applies to the records at issue, which were created after the ORCS was approved. There clearly is a need to develop a schedule to govern the retention of these records.

RECOMMENDATION 6:

The Ministry should apply to amend its ORCS to include a new schedule that governs data extracted from its Educational Data Warehouse. The designated retention period should be the minimum amount of time required for operational purposes.

4.6 TRAINING

The CPPM and ISP provide a robust set of guidelines on how to inventory and secure personal information and devices used to store personal information.

In 2011, government initiated mandatory privacy training for all government employees. My office's *An Examination of BC Government's Privacy Breach Management* report notes that training was intended to inform "employees about [their role] and responsibility in handling personal information and preventing information incidents."[18] At the time I issued this report in 2015, only 70.9% of government employees had received privacy training. As of December 2015, 90% of Ministry of Education employees had completed mandatory privacy and information sharing awareness training.

Based on the interviews, the employees involved did have some basic knowledge of the policy set out in the CPPM and the ISP. They were aware that encryption of mobile storage devices was required by policy. One witness raised concerns about storing the backup hard drive off-site.

Nevertheless, the overriding concern here is that the employees did not follow the policies. Whether the reason was lack of awareness or the belief that they could contravene the policies as long as they provided alternative security arrangements, the result was the contravention of policies led directly to the privacy breach. In this case, the widespread violation of policy by staff and managers indicates that the training at the time was not effective in ensuring compliance with policies necessary to protect the personal information.

[18] [2015] B.C.I.P.C.D. No. 65.

RECOMMENDATION 7:

To ensure that Ministry employees follow the policies and procedures necessary to comply with s. 30 of FIPPA, they should receive mandatory training with periodic refresher courses on the collection, use, disclosure, security and retention of personal information and why it is essential that they comply with government policy.

4.7 AUDIT

This report demonstrates that government must do more than just develop sound policy. It must enforce these policies more effectively. After issuing policies and training employees on how to comply with them, it is necessary to follow up to measure compliance.

Periodic internal audits are an integral component of managing privacy. Internal audit processes ensure employee compliance with CPPM, ISP and FIPPA.

Audits based on pre-arranged schedules may include, for example,

- interviews with employees;
- review of files;
- review of data dictionaries; and
- examination of technical and physical security measures.

Internal audits are an effective mechanism for early identification of potential threats to the security of personal information. In this case, a timely audit may have helped to avoid the breach. However, the lack of an inventory may have hampered the effectiveness of such an audit. This reinforces the need for an accurate and up to date inventory.

In my report *An Examination of BC Government's Privacy Breach Management*, I noted that an internal audit program that monitors compliance is essential for an effective privacy breach management program.[19] While the government has indicated an intention to implement such a program, one was not in place at the time of the events outlined in this report.

[19] [2015] B.C.I.P.C. D. No. 65, p. 35.

RECOMMENDATION 8:

The Ministry should implement an audit program that includes risk assessments to evaluate the security of personal information, audits against policy, and reviews the effectiveness of staff training.

SUMMARY

The government had a reasonable and adequate policy framework in place to assist it in meeting the requirements of s. 30 of FIPPA, but the Ministry failed to ensure that it was effective in protecting the personal information at issue. Ministry employees contravened these policies several times.

Ministry employees made a series of statutory and policy contraventions that resulted in the breach. The decision to retain the personal information in the project files indefinitely created a privacy liability. The placing of the personal information on the portable hard drives was a contravention of policy that put the personal information of millions of children at risk. The failure to ensure the drives were encrypted compounded that risk. Moreover, the decision to store one of the drives off site at a warehouse that was not an approved storage facility was a further contravention that led to the backup hard drive going missing. I also find that the Ministry failed to inventory the information on the drives as required by FIPPA. Had the employees followed the appropriate policy at just one of these stages, they likely would have been able to avoid the breach.

FINDING

I find that, at the time of the events outlined in this report, the Ministry did not have reasonable security arrangements in place, as required by s. 30 of FIPPA, to protect the personal information in the project files stored on the portable hard drives.

The Ministry also failed to meet its obligation under s. 69(3) of FIPPA to keep a summary of all the personal information banks located on the portable hard drives.

5.0 RESPONSE TO THE PRIVACY BREACH

Issue 2: Did the Ministry take reasonable steps in response to the privacy breach as required by s. 30 of FIPPA?

5.1 What is a Privacy Breach?

A privacy breach includes loss of, unauthorized access to or unauthorized collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" in British Columbia, if it occurs in contravention of FIPPA. Privacy breach management is a key component of a public body or organization's overall privacy management program.

A public body's obligations under s. 30 include the actions it takes when there has been a privacy breach. Managing breaches forms part of the duty to protect personal information.[20] OIPC investigation reports and guidance documents highlight a need for appropriate and effective privacy breach management;[21] timely notification of affected individuals;[22] and due consideration for reporting breaches to the OIPC in order for entities to meet their legislative obligations.[23i]

In his report into a breach involving browsing by an employee of a service provider to the Ministry of Small Business and Revenue, former Commissioner Loukidelis outlined what a public body must do when responding to a privacy breach:

> In order to assist public bodies, the OIPC has published a key steps document for managing privacy breaches. When a privacy breach occurs, public bodies and service providers need to make every reasonable effort to recover the personal information, minimize the harm resulting from the breach and prevent future breaches from occurring. The OIPC's key steps document has been useful in our review and evaluation of the Ministry's

[20] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, pp. 14, 15. (https://www.oipc.bc.ca/guidance-documents/1545).

[21] Office of the Information and Privacy Commissioner. Investigation Report F06-02, para. 81. (www.oipc.bc.ca/investigation-reports/1233).

[22] Office of the Information and Privacy Commissioner. Investigation Report F06-02, para. 55. (www.oipc.bc.ca/investigation-reports/1233).

[23] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in BC's Public Sector*, pp. 14-15. (https://www.oipc.bc.ca/guidance-documents/1545). Office of the Information and Privacy Commissioner. 2012. *Privacy Breaches: Tools and Resources*, pp. 7-9. (http://www.oipc.bc.ca/guidance-documents/1428).
Office of the Information and Privacy Commissioner. 2013. *Accountable Privacy Management in BC's Public Sector*. https://www.oipc.bc.ca/guidance-documents/1545.
Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioners of Alberta and Office of the Information and Privacy Commissioners of British Columbia. 2012. *Getting Accountability Right with a Privacy Management Program.* https://www.oipc.bc.ca/guidance-documents/1435.

> actions in this case. The four key steps public bodies must undertake in managing a privacy breach are:
>
> 1. Contain the breach;
> 2. Evaluate the risks;
> 3. Determine whether notification of affected individuals is required; and
> 4. Develop prevention strategies to reduce risks in the future.
>
> The first three steps should occur as soon as possible following the breach, either simultaneously or in quick succession.[24]

This report structures its assessment of the Ministry's response around these four key steps.

5.2 CONTAINMENT

Once the Ministry discovered that the backup hard drive was not in the locked cage at the warehouse, it commenced an extensive search. By the time the incident had been reported to the OIPC, a team of employees had searched several possible locations for the backup hard drive multiple times:

- **Warehouse**: the Ministry searched the warehouse cage before and after reporting the missing backup hard drive to OCIO. It conducted successive searches including all Ministry materials held at the warehouse. There were four unsuccessful searches of the warehouse, with the final search being a complete search of every room and storage area located in the entire facility.

- **Workplace**: the Ministry searched the work unit offices at 620 Superior including common spaces, staff lockers, locked drawers and cabinets, and remaining private spaces.

- **Ministry of Advanced Education, St. Ann's Academy**: the Ministry searched three safes and other storage areas at St. Ann's.

- **Records Management Files**: Ministry staff conducted a review of disposal records since 2009 and off-site storage records to determine whether the backup hard drive had been disposed of or sent to another facility.

- **General Education Development (GED)**: There was a concern that the backup hard drive may have moved with the GED exams to the GED office in Washington, D.C. The Ministry contact confirmed that the backup hard drive was not sent with the GED material.

[24] Investigation Report F07-01, [2007] B.C.I.P.C.D. No. 13, p.8.

The Ministry spoke to past and present employees who may have had some knowledge of the location of the drive.

The Ministry created a timeline report, which thoroughly documented their efforts to locate the drive. This was of great assistance in the conduct of this investigation.

The backup hard drive has not been recovered.

FINDING

I find that the Ministry took all reasonable steps to contain the breach following the discovery that the backup hard drive was missing.

5.3 RISK EVALUATION

The hard drives contained varying levels of personal information for 3.4 million students and teachers from 1986 through 2009. The detail and sensitivity of personal information varied depending on the group to which the individual belonged.

The following personal information for 3,166,388 BC and Yukon students and all applicants to public post-secondary institutions from 1991 to 2009 was stored on the backup hard drive:

- full name, date of birth;
- home postal code that year;
- PEN;
- home address for Grade 12 students being mailed their transcript; and
- the name of the community of the student's latest home address.

There were a number of subgroups who had additional personal information on the backup hard drive. The groups are described as:

- 1991-2009: K-12 students (1,850,044)
- 1990: Middle school students in Grades 6, 7, 8 (3,457)
- 1986-1989: Grade 12 students (188,322)
- 1991-2008: All student exams and course information
- 1991-2008: All Yukon student exams and course information
- 1999-2008: Foundation Skills Assessment for students Grades 4, 7 & 10
- 2008: tracked students who withdrew from Grade 12 (200)
- 1993-2008: Yukon exam results – (1,300)
- 2007: Yukon distributed learning – selected individuals (162)

- 2007-2008: Yukon student graduation files (370)
- 2003: Teachers' retirement survey (825)
- No date: Teachers correspondence that is sometimes of a personal nature (169)
- 2006: Teacher and school staff attending the 2006 Annual Teacher Congress (342)
- 2002-2009: Individuals enrolled in public Post–Secondary institutions (511,945)
- K-12 achievements – background for K-12 graduates who did not attend Post-Secondary institutions
- 2000-2008: Students applying for and receiving financial aid (252,000)
- 2008: Public Post-Secondary cancer survivors involved Post-Secondary research trial (1,052)
- 2005-2008: Students enrolled in industry training program (6,700)
- 2006-2007: Children receiving Ministry of Children and Family Development ("MCFD") services (9,273)
- 2001-2007: MCFD Children under custody orders (8,170)
- 2000: MCFD children in care (10,125)

The personal information found within each group varies in level of sensitivity. The most sensitive information was in the MCFD files and files containing information about students with special needs. Examples of personal information from these subgroups include:

- Special needs type
- Intervention specifics
- Reasons for school withdrawal (e.g., drug use, mental health, family problems)
- Names of students receiving financial aid
- Supervision status for MCFD supported students

There was no financial, banking or pension information on either hard drive.

The Ministry, with the advice and assistance from the OCIO, identified a number of privacy risks depending on the types of personal information associated to each group. The primary risks for the majority of individuals were identity theft and fraud. Given the limited nature of the information on the drive and the lack of any financial information or the SIN, the Ministry considered these risks to be low. The Ministry identified the following possible additional harms: emotional hurt, humiliation or damage to reputation, particularly with reference to those students from the listed subgroups.

While the Ministry correctly identified these additional harms for the subgroups, I believe that it is important to appreciate that the privacy risks in this case go even further. I think it essential to emphasize that the affected individuals are some of the most vulnerable in our society. They include children in care, children in custody, children with special needs, and children with health conditions. These are all circumstances that can lead to stigmatization by society in general and instances of individual discrimination. I conclude that the risk assessment meets the minimum standard but was not as thorough as possible.

FINDING

I find that the privacy risk evaluation performed by the Ministry was adequate.

5.4 NOTIFICATION

The Ministry concluded that the risks of emotional hurt, humiliation and damage to reputation warranted direct notification where possible.

The Ministry first considered directly notifying all individuals. However, there were 2.75 million individuals for whom it did not have either reliable address information or any address information. Therefore, the Ministry decided to conduct indirect notification for all affected individuals. On September 22, 2015, the Ministry issued a notice through the media in an attempt to alert individuals whose personal information may have been contained on the backup hard drive.[25]

The news release described the types of information that was on the backup hard drive. It identified individuals who may be affected by the breach.
It advised readers that the Ministry was investigating the loss of the backup hard drive. It provided government contact information and a web link for affected individuals who might have further questions. It recommended affected individuals scrutinize their financial records for indicators of identity theft.
The notification also provided contact information for credit monitoring services.

In addition, the Ministry decided to directly notify as many as possible of the individuals whose personal information contained additional details that were sensitive.

The Ministry identified the following groups as warranting direct notification:

- Children who withdrew from school;
- Teachers who completed the retirement survey;
- Youth with special needs;

[25] http://www2.news.gov.bc.ca/news_releases_2013-2017/2015MTICS0026-001575.htm.

- Students receiving financial loans; and
- Students who had survived cancer.

The Ministry only has address information for 146,310 individuals in the above listed groups. The Ministry identified 25,550 individuals whose addresses have a reasonable chance of being accurate. The remainder were rejected as non-valid addresses. On January 22, 2016, the Ministry sent generic notification letters to those individuals. The letters informed them that their information was included in the breach and provided a website link with further details.[26]

The Ministry also plans to directly notify those approximately 3,000 individuals identified as receiving MCFD support or supervision. The Ministry is working with MCFD to obtain reasonably current addresses. In collaboration with MCFD, it is conducting a balance of harms assessment. Once this is complete, the Ministry will directly notify appropriate individuals. The Ministry believes that this process will take several more months to complete.

I note that there has been a considerable delay in carrying out the direct notifications. Normally, a delay of five months from the discovery of the breach would be unacceptable and would compromise the ability of the affected individuals to mitigate any potential harm. Nevertheless, in this case, as the breach occurred sometime during the last five years, it is unlikely that earlier notification would have improved the situation that the affected individuals face. Moreover, the Ministry did provide indirect notification in a timely manner.

With respect to direct notification, it is my view that, while the speed with which it is undertaken should be accelerated, the process itself meets the requirements of s. 30 of FIPPA.

RECOMMENDATION 9:

Ministries should ensure that they conduct direct notification of affected individuals without delay, even in cases where there is not compelling urgency for immediate notification.

FINDING

I find that the indirect notification through the media release combined with the completed and proposed direct notifications will meet the requirements of s. 30 of FIPPA with respect to notification.

[26] http://www.cio.gov.bc.ca/local/cio/priv_leg/documents/reports/Education_Data_Breach.pdf.

6.0 PREVENTION STRATEGIES

The Ministry has taken a number of steps to reduce the risk of a similar breach occurring. First, it has transferred the data from the office-use hard drive to the SSBC server. The office-use hard drive was handed over to the OCIO for the purpose of the breach investigation. Once the Ministry of Finance is satisfied there is no further need to retain the hard drive, it will be securely destroyed.

Second, on December 14, 2015, the Ministry implemented a policy requiring that all portable storage devices, which include external hard drives and USB flash drives, are hardware encrypted to government standards, regardless of the content.

Third, it is inventorying and documenting the types of information stored on all mobile storage devices. The purpose of this process is to ensure that mobile storage device use is consistent with government policy.

Fourth, government is in the process of implementing its Privacy Management and Accountability Policy ("PMAP"). The Ministry is adopting PMAP, including appointing a Ministry Privacy Officer. The Privacy Officer will initiate personal information inventories, compliance policies, conduct internal audits and provide continuous privacy training to employees.

FINDING

I find that, on balance, the Ministry took reasonable steps in response to the privacy breach that met its requirement to provide adequate security to personal information under s. 30 of FIPPA.

FINDING

The Ministry has taken reasonable steps to reduce the risk of similar breaches from occurring.

7.0 SUMMARY OF FINDINGS AND RECOMMENDATIONS

7.1 SUMMARY OF FINDINGS

1. **I find that, at the time of the events outlined in this report, the Ministry did not have reasonable security arrangements in place, as required by s. 30 of FIPPA, to protect the personal information in the project files that were stored on the portable hard drives.**

   The Ministry also failed to meet its obligation under s. 69(3) of FIPPA to keep a summary of all the personal information banks located on the portable hard drives.

2. **I find that the Ministry took all reasonable steps to contain the breach following the discovery that the backup hard drive was missing.**

3. **I find that the risk evaluation performed by the Ministry was adequate.**

4. **I find that the indirect notification through the media release combined with the completed and proposed direct notifications will meet the requirements of s. 30 of FIPPA with respect to notification.**

5. **I find that, on balance, the Ministry took reasonable steps in response to the privacy breach that met its requirement to provide adequate security to personal information under s. 30 of FIPPA.**

6. **The Ministry has taken reasonable steps to reduce the risk of similar breaches from occurring.**

7.2 SUMMARY OF RECOMMENDATIONS

1. **Ministry staff should be reminded that they must store personal information securely. Complying with the requirement to consult with their MCIO on relevant policy and procedures before making decisions regarding the secure storage of personal information and with CPPM 6.3.5 when purchasing portable storage devices will assist in meeting the Ministry's statutory obligation under FIPPA.**

2. **The Ministry should comply with the requirement in s. 69 of FIPPA to maintain an accurate inventory of personal information assets in the directory of Personal Information Banks, including all personal information stored on portable storage devices.**

3. **To assist with meeting the statutory requirement to store personal information securely, the Ministry should comply with CPPM policy and the OCIO directive 44692 and transfer all personal information from portable storage devices on to the government network as soon as practicable and delete the personal information from the devices.**

4. **To assist with meeting the statutory requirement to store personal information securely, the Ministry should comply with the requirement that when securing mobile devices off-site, they store them in a government approved storage facility, which would document the handling of the device.**

5. **To assist with meeting the statutory requirement to store personal information securely, the Ministry should ensure that it complies with ISP and CPPM policies regarding encryption. If it stores personal information on mobile data storage devices, it must encrypt those devices.**

6. **The Ministry should apply to amend its ORCS to include a new schedule that governs data extracted from its Educational Data Warehouse. The designated retention period should be the minimum amount of time required for operational purposes.**

7. **To ensure that Ministry employees follow the policies and procedures necessary to comply with s. 30 of FIPPA, they should receive mandatory training with periodic refresher courses on the collection, use, disclosure, security and retention of personal information and why it is essential that they comply with government policy.**

8. **The Ministry should implement an audit program that includes risk assessments to evaluate the security of personal information, audits against policy, and reviews the effectiveness of staff training.**

9. **Ministries should ensure that they conduct direct notification of affected individuals without delay, even in cases where there is not compelling urgency for immediate notification.**

8.0 CONCLUSIONS

The key message in this report is that, while it is essential to have strong privacy and security policies, these policies alone are not sufficient to constitute reasonable security measures. The government had clear and appropriate policies in place that would have prevented the breach, if Ministry employees had followed them. These employees had received privacy training and appeared to be aware of the policies, but they did not abide by them.

Public bodies need to take appropriate steps to verify that employees are complying with these policies. They must ensure that their employees are aware of these policies, understand them, and appreciate the consequences of contravening them. I have previously noted the essential role of audit and compliance monitoring as part of an effective privacy management program. Public bodies must have a comprehensive training plan supported by audits and spot checks.

Identifying prevention strategies is a key component of the four step process of responding to privacy breaches. Again, the formulation of these strategies is not enough. Public bodies must ensure that the strategies are implemented and followed. The data breach involving the sale of computer tapes containing personal information led to an OCIO directive with respect to mobile storage devices. However, no one at the Ministry made sure that its employees were complying with this directive. Had they been in compliance, they would have avoided this breach because they would not have stored the data on portable hard drives in the first place.

This is another example of the importance of executive leadership. The Ministry executive should communicate clearly to employees that corporate information policies are mandatory, not optional. Information assets are as important as financial assets. They should support effective training and compliance monitoring programs. There is a suggestion that the decision to transfer the data to the portable hard drives was the result of a financial imperative to divest the SSBC servers of as much data as possible. Both Ministry executive and employees need to be clear that financial imperatives are not an acceptable justification for blatant contraventions of corporate policy that put personal information at risk.

The OIPC will be following up with the Ministry in three months for an update on how it is implementing the recommendations in this report.

9.0 ACKNOWLEDGEMENTS

The Ministry of Education cooperated fully with our investigation.

I would also like to thank Jay Fedorak, Deputy Registrar/Assistant Commissioner, Tim Mots, Investigator and Tanya Allen, Senior Investigator, Audit and Compliance, who conducted this investigation and contributed to this report.

January 28, 2016

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

APPENDIX A – Cited Policies and Directive

Core Policy and Procedure Manual

6.3.5 Information Management and Information Technology (IM/IT) Procurement

a. General

1. Previous approval requirements are superseded by Treasury Board Directive 5/04 (February 4, 2004).
2. All IM/IT goods and services must be procured in accordance with the business requirements of the ministry as identified in the Ministry Service Plan.
3. Prior to initiating procurement of all IM/IT-related products or services, ministries must discuss their IT requirements with Procurement Services Branch, SSBC and their IM requirements with the Chief Information Office (CIO), which will determine whether a corporate solution will be implemented for the requirement.
4. Large projects frequently include smaller IM/IT-related component projects. These component projects must be considered at the same time as the larger project.
5. All IM/IT goods and services must be procured in accordance with government financial and procurement policies, including the Core Policy and Procedures Manual, and must be consistent with the ministry Information Resource Management Plan, the Agreement on Internal Trade, and the Chief Information Office (CIO) policies, strategies and standards, and all legislative requirements.
6. All ministry IM/IT hardware and software requirements, including shared devices (e.g., desktop, laptop, server, and printer devices) must be ordered through SSBC. Where available, CSAs, pre-established by SSBC, will be utilized for the supply of these items. Any exceptions to this policy must be approved by CIO, or SSBC, as appropriate. This policy applies to purchases of any volume or dollar value.

12.3.3 Information Management

Part II: Personal Information Protection Policy

a) Privacy Impact Assessments

1. A Privacy Impact Assessment (PIA) must be conducted to determine if a project, program, application, system or new enactment collects, uses, retains or discloses or secures personal information.
2. A preliminary PIA must be completed during the feasibility or initiation stage of any project, program, application, system or enactment. A formal PIA must be finalized, including the sections on security and retention of personal information, before implementation of any project, program, application, system or enactment.

3. Ministries must review existing summaries in the government Personal Information Directory, PIA section, at least once a year, and submit new summaries as needed within 30 days of the final signing off of a PIA.

b) Information Sharing Agreements

1. Ministries must develop Information Sharing Agreements to cover personal information exchanges outside of the immediate program area, as required. These agreements must include a compliance review requirement and schedule of planned reviews.
2. Ministries must review existing sharing agreement summaries in the government Personal Information Directory, Information Sharing Agreement section, at least annually, and submit new summaries as needed within 30 days after approval of an Information Sharing Agreement.

c) Personal Information Banks

1. Ministries must maintain a directory of Personal Information Banks and review the existing Personal Information Banks summaries in the government Personal Information Directory at least annually.

New Personal Information Bank summaries must be submitted to the government Personal Information Directory within 30 days of implementation.

Part III: Managing Information

a) Governance of Recorded Information

1. government must manage all records created and received during the conduct of its business activities.
2. Ministries must establish and maintain a recorded information management program.
3. Ministries must establish and maintain a forms management program.
4. government records must be managed and preserved to remain authentic, reliable, trustworthy, secure, complete and accessible over time and location regardless of media or format.

Ministries transferring records to off-site storage must use approved records centres.

12.3.6 Information and Technology Security

a) Security

1. A formal management framework will be established to initiate, implement, monitor and enforce information and technology security within the government of British Columbia.
2. Security requirements must be assessed, identified and documented to determine security implications and control requirements when there is a requirement for third parties to access government assets. Security controls must be documented and agreed to with the third party.
3. Information and technology assets must be classified, inventoried and recorded with an identified owner who is responsible for achieving and maintaining appropriate protection of those assets.
4. Users of government assets must continue to be aware of, and understand, their role in reducing the risk of theft, fraud or misuse of government assets. Changes in responsibilities, roles, contracts or employments must be managed.
5. Operating procedures must be documented and monitored to ensure the correct and secure operation of information and communication technologies.

6. Third party service delivery agreements must be monitored for compliance, and changes managed to ensure that the services delivered meet or exceed specified requirements.
7. Operational requirements for new systems must be established, documented and tested prior to acceptance and use. Future capacity requirements should be made to reduce the risk of system overload or failure.
8. Documents, computer media, data and system documentation must be protected from unauthorized disclosure, modification, removal or destruction.
9. Data and information exchanges within government, or with an external entity, must be secure and managed through a documented process.
10. government information and technology assets will be monitored regularly and logs maintained to identify inappropriate access, use, or other security events.
11. Access to information, systems, and business processes must be managed and controlled on the basis of business and security requirements.
12. Access to, or from, internal and external networks and network services must be managed and controlled.
13. Security requirements must be assessed, identified, documented, and agreed to during all stages of development.
14. The security controls of new or modified information systems and services must be reviewed prior to implementation.
15. Information and technology assets will be protected commensurate with the identified risks and security requirements.
16. Information security incidents, events and weaknesses must be managed and communicated to the government Chief Information Officer for corrective action, if appropriate.
17. Information security management requirements must be integrated into the business continuity planning process to protect information systems and communication technologies from disasters, loss of service or information security failures.
18. The security of information systems and communications technologies must be regularly reviewed to ensure compliance with applicable legislation, policies, standards and documented security controls.

Information Security Policy

6.7.1 All removable computer media must be managed with controls appropriate for the sensitivity of the data contained on the media.

a) Management of government records
b) Use of portable storage devices
c) Human factors
d) Risk assessment factors and controls
e) Mandatory controls

Purpose: To ensure that *risks* to information introduced by *portable storage devices* are sufficiently managed.

6.7.1 a) Management of government records

Information Access Operations, Shared Services BC is responsible for the management and disposal of government records through the *Document Disposal Act.*

6.7.1 b) Use of portable storage devices

The use of portable storage devices to store or transport information increases the risk of information compromise. Portable storage devices are typically small, portable and are easily lost, stolen or damaged, particularly when transported in public environments. *Information Owners*, *Information Custodians and Managers* must:

- Ensure that use of portable storage devices is managed and controlled to mitigate risks;
- Document processes for authorizing use of portable storage devices; and,
- Ensure personnel using portable storage devices protect information and information technology assets in their custody or control.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity, a *Security Threat and Risk Assessment* must be performed prior to permitting the use of a class of portable storage devices.

Technical standards for each class of media must be documented including product name, mandatory controls, permitted information classifications and strength of controls such as encryption key length.

Media handling procedures should include instructions to minimize the amount of information stored on portable storage devices.

6.7.1 c) Human factors

Information Owners, *Information Custodians and Managers* must ensure personnel using portable storage devices are:

- Aware of the additional risks and responsibilities inherent with portable storage devices;
- Familiar with operation of the required protection technologies and when they must be used; and,
- Familiar with security event and loss reporting procedures.

6.7.1 d) Risk assessment factors

The Security Threat and Risk Assessment must consider the impact of disclosure or loss of information stored on portable media from threats such as:

- Loss or physical theft;
- Limited ability to control and log access to stored data;
- Accidental media destruction;
- Improper long term storage environment;
- Exposure to malicious and mobile code; and
- Incomplete erasure of data prior to device disposal.

Information classification and sensitivity levels must be considered in the risk assessment.

6.7.1 e) Mandatory controls

Minimum information protection safeguards for the use of portable storage devices include:

- Disabling portable storage devices, media drives or connection ports where no business reason exists for their use;
- Documented definition of information classifications or sensitivities permitted to exist on specific media types;
- Not storing the only version of a document on portable storage devices;
- Documented authorization processes for use of portable storage devices;
- Encryption of stored data;
- Contractual requirements for external parties that transport, handle or store portable storage devices;
- Adherence to manufacturer specifications for media storage environment; and,
- Documented portable storage devices handling procedures including:
    - Off-site storage,
    - Third party transportation,
    - Information backup,
    - Prevention of mobile and malicious software,
    - Logging of media custody and location to allow for accounting and audit,
    - Media labelling to indicate owner, classification and special handling restrictions,
    - Maintenance of information where the information storage requirement exceeds the expected media lifetime, and,
    - Secure erasure and disposal.

…

Only approved media devices appropriate for the classification of the information being stored may be used.

7.7.1 Appropriate controls must be implemented to mitigate security risks associated with the use of portable storage devices.

a) Information protection paramount
b) Service-specific risks and practices
c) Protection of credentials
d) Protection of network endpoint and physical device
e) Human factors
f) Risk assessment factors

Purpose: To protect information stored on *portable storage devices* from loss or unauthorized access.

7.7.1 a) Information protection paramount

Information Owners and Information Custodians must ensure that use of portable storage devices is managed and controlled to mitigate the inherent *risks* of portable storage devices.

The use of portable storage devices such as laptops or other mobile devices to access, store, or process information increases the risk of information compromise. Portable storage devices are typically small, portable, used in uncontrolled public environments and are easily lost, stolen or damaged.

To ensure that sufficient safeguards are implemented to protect information commensurate with its sensitivity a *Security Threat and Risk Assessment* (STRA) must be performed prior to permitting subscription or use of *mobile computing services.*

Users of mobile computing services must ensure that information and information technology assets in their custody or control are protected.

7.7.1 b) Service-specific risks and practices

Providers of mobile computing services must perform annual risk assessments to identify service-specific risks. Policies, standards, practices and guidelines that treat these risks must be developed, documented and maintained by the service provider.

7.7.1 c) Protection of credentials

User identifiers and user credentials must be protected to reduce the risk of unauthorized access to information and information technology assets.

In particular, users must protect against visual eavesdropping of passwords, PINs and other credentials, especially when in public places. See ISP 7.3.1

7.7.1 d) Protection of network endpoint and physical devices

Portable storage devices are typically used to store information or remotely access *government networks* and services. The policies and procedures governing *remote access* apply to mobile devices. See ISP ss. 6.6.1, ISP 7.4.1, ISP 7.4.2, ISP 7.4.5 and ISP 7.4.6. Where Remote Access services are used, the portable storage device must be configured to prevent its use as a conduit between the non-government and government networks (e.g., VPN split tunnelling must be disabled).
Network access to portable storage devices from non-government networks must be blocked by implementation of firewall or filtering technologies to protect against attack (e.g., to prevent network attacks against the mobile device).

Portable storage devices must be protected against *mobile* and *malicious code*.

Portable storage devices must be locked and/or secured when unattended to prevent unauthorized use or theft (e.g., use device locks, cable locks, physical container locks, PINs or screensaver locks).

7.7.1 e) Human factors

Information Owners and Information Custodians must provide users of mobile computing services with security awareness training, to ensure that Users are:

- Aware of the additional risks and responsibilities inherent in mobile computing and when using portable storage devices;
- Familiar with operation of the protection technologies in use; and,
- Familiar with the Information Incident Management Process.

7.7.1 f) Risk assessment factors

The Security Threat and Risk Assessment must consider threats to information and information technology assets, such as:

- Physical theft;
- Use of the portable devices to remotely access government networks and systems;
- Data interception;
- Credential theft;
- Unauthorized device use;
- Device destruction;
- Information destruction;
- Covert key logging or password harvester programs; and,
- Malicious and mobile code.

Information classification and sensitivity levels must be considered in the risk assessment.

Minimum information protection safeguards for the use of portable storage devices include:

- **Encryption of stored data** to prevent information loss resulting from the theft of the mobile or remote device;
- **Encryption of data transmitted** via public network;
- **Access control permissions on a portable storage device** must be applied to prevent unauthorised access to information by system users, particularly for multi-user mobile systems;
- **Regularly maintained data backups** of information stored on portable storage devices using government backup facilities to protect against information loss;
- To provide **information availability** portable storage devices must not be used to store the only copy of a government record;
- **Physical security of the device** must be maintained to protect against asset and information loss; and,
- **User authentication** to the portable storage device and **user authentication** for remote

Portable Storage Directive

Memorandum 44692 – Use of Portable Storage Devices

Ref: 44692 **VIA e-MAIL**
Date: June 2, 2006
To: Assistant Deputy Minister of Corporate Services
Re: Use of Portable Storage Devices

In regards to the “Investigation Report 2006 – 048 – Loss of custody of 41 computer data tapes containing personal and sensitive information”, recommendation number 7 (attached) describes the need to store sensitive or personal information on the government network and not on “non-encrypted” portable storage devices (e.g., disks, memory sticks, MP3 players, CDs/DVDs) or local hard drives. In support of this recommendation:

- management, employees and contractors are to be reminded that they are responsible for the information and storage devices under their care;
- information temporarily stored on a portable storage device should be transferred to the government network as soon as practicable and then deleted from the portable storage device. government information should be stored on the government network whenever possible to ensure the protection and long term availability of the information;
- sensitive or personal information must be encrypted when stored on portable storage devices to ensure protection from loss, compromise or unauthorized disclosure. Staff should ensure that information in their care is protected commensurate with its value and sensitivity; and
- government policy (Core Policy and Procedures Manual 6.3.5(a) 6)) requires that all information technology hardware purchases be handled by Shared Services BC (CITS). I have asked Shared Services BC to temporarily stop issuing memory sticks until a suitable encryption mechanism can be identified and implemented. Ministries can contact their Client Business Analyst for advice on short term alternatives to the use of memory sticks and exception processes.

As part of recommendation number 5 (attached), Mr. Bruce Cuthbert and Mr. Brent Grover from my office are conducting a feasibility study on the encryption of portable storage devices and backup storage devices to protect government data. Results of this study will be used to select encryption products and processes to ensure the protection of government’s information assets.

[Office-use Signed By:]

Dave Nikolejsin
Chief Information Officer

Attachment

cc: Mr. Gordon Macatee, Deputy Minister
Ms. Elaine McKnight, Assistant Deputy Minister

Assistant Deputy Ministers of Corporate Services, Advisory Council
Information Management
Mr. Bruce Cuthbert, Director, ICT Architecture & Standards
Mr. Brent Grover, Manager, IT/IM Policy

Attachment

Excerpt from "Investigation Report 2006 – 048 – Loss of custody of 41 computer data tapes containing personal and sensitive information"

Recommendation number 5
It is recommended that government consider the feasibility of encrypting government data on portable storage devices (e.g., Blackberries, laptops, etc.) and on backup storage devices.

Recommendation number 7
It is recommended that government issue policy that all computer files containing personal information be stored on the government network and not on "non-encrypted" personal computing devices or data storage media (e.g., personal computer hard drives, laptops, PDAs, etc.).