Office of the
Saskatchewan Information
and Privacy Commissioner

INVESTIGATION REPORT 072-2018

Ministry of Central Services

March 8, 2019

Summary: The Commissioner undertook an investigation of the Ministry of Central Services' use of backup tape technology and the potential issues posed by this technology, as it relates to conforming with the requirements of *The Freedom of Information and Protection of Privacy Act* (FOIP). The focus of the investigation is on the critical data that Central Services copies onto backup tapes and an assessment of how FOIP applies to such data, as well as how Central Services manages backup tapes. This investigation did not include the broad records and information management issues that fall under the prevue of the Provincial Archives of Saskatchewan; however, the Provincial Archives received a copy of this report and they support the findings and recommendations in this report. The Commissioner made several findings including that, with some exceptions, backup tapes do not need to be included in a search for responsive records when an application under FOIP exists and that the requirements of section 24.2 of FOIP apply to the management of all backup tapes. The Commissioner made a number of recommendations to Central Services, some of which that are expected to be implemented within one year of issuance of this report.

I BACKGROUND

[1] Over the last few years, I have been following the evolution of backup tape technology and its use within the Government of Saskatchewan. I have noticed, based on reviews conducted by my office, complaints received and articles published on the topic, that there appears to be a shift from the original purpose and use of backup tape technology, and that

this shift has resulted in challenges with conforming to the access and privacy-related requirements in the province. I have also noted that the current state of Government of Saskatchewan information stored on backup tapes could be a concern because of the reported deteriorating nature of this media. For these reasons, I have decided that it is time my office take a closer look at the use of backup tape technology and the potential issues posed by this technology.

[2] As the responsibility for managing backup tapes containing government information falls within the mandate of Central Services, I met with Central Services officials on March 26th, 2018. The purpose of this meeting was to obtain general information on the backup tape technology in use and the retention and disposition of records and data stored on backup tapes.

[3] Following that meeting, on April 24th, 2018, I notified Central Services of my intention to review matters related to backup tape technology, in accordance with section 33 and subsection 45(2) of *The Freedom of Information and Protection of Privacy Act* (FOIP). These sections provide:

> **33** The commissioner may:
>
> (a) offer comment on the implications for privacy protection of proposed legislative schemes or government programs;
>
> (b) after hearing the head, recommend that a government institution:
>
> (i) cease or modify a specified practice of collecting, using or disclosing information that contravenes this Act; and
>
> (ii) destroy collections of personal information that is collected in contravention of this Act;
>
> …
>
> (d) from time to time, carry out investigations with respect to personal information in the possession or under the control of government institutions to ensure compliance with this Part.
>
> **45(2)** The commissioner may:

> (a) engage in or commission research into matters affecting the carrying out of the purposes of this Act;
> …
> (c) receive representations concerning the operation of this Act;

[4] My office's investigation was conducted from April 24th, 2018 to December 5th, 2018. During this time, officials from my office participated in various meetings involving Central Services officials, obtained and reviewed documents related to the management of backup tape technology, including various policies and procedures, and visited two of the storage facilities where backup tapes are kept.

[5] I would like to thank the members of the Operations Team within the IT Division at Central Services – who are responsible for overseeing the management of backup tapes – the Chief Information Officer and the designated Audit Liaison Officer, for the cooperation extended during this investigation.

About Central Services

[6] Central Services is the major internal service provider for the Government of Saskatchewan. In accordance with the *Ministry of Central Services Regulations, 2016*, Central Services can develop, promote and implement policies and programs relating to information technology, information management and records management. This broad mandate allows Central Services to offer a range of IT services, including backup and recovery of data.

[7] At the time of writing this report, Central Services was providing backup and recovery services to twenty-seven ministries and agencies, both within and outside the Executive Government. Annex A of this report provides a complete list of these ministries and agencies. Central Services has confirmed that a Service Level Agreement between their institution and each of its clients exists to outline the services provided by Central Services.

[8] Central Services has been working toward using a "tapeless" backup technology service, based on a service provided by a third party, Actifio. This new tapeless service will significantly reduce the time required to recover information in case of a disaster or IT disaster and will eliminate the need for the use of backup tapes. The service has been fully functional since October 2017, though there is still some work to be done before backup tapes can be eliminated.

Management of Backup Tapes

[9] For the purposes of this investigation, a backup is a copy of files and programs saved onto physical backup tapes resembling old VHS cassette tapes (see Figure 1 below). These backup tapes facilitate the recovery of files and programs should there be an unexpected and significant disruption, like a natural disaster or Information Technology (IT) system failure. The value of using backup tapes is that they can store enormous amounts of data in a relatively compact format. This makes them a cost effective method of storing large volumes of data. Data archival is sometimes confused, or used interchangeably, with backups for recovery purposes. Archiving exists for a different purpose, namely to remove or duplicate files from an active system to another system or digital media for short or long-term storage.

[10] Email archiving, another term often confused with backups for recovery purposes, can help to process and file emails systematically. Archiving emails primarily serves the purposes of allowing emails to be retrievable and made available over a longer period. Archiving emails ensures they are stored securely and their contents remain unchanged.

[11] Central Services relies on a third-party service provider, ISM Canada, to oversee the day-to-day management of backup tapes and their offsite storage. ISM subcontracts some of the management to another third party, Crown Store-All. ISM provides Central Services with reports on the movement into, and out of, backup storage facilities and maintains an annual log of all backup tapes.

[12] The Operations Team within the IT Division at Central Services is the team responsible for overseeing the management of backup tapes and working with the third-party service providers who provide services to Central Services under contracts.

[13] Although Central Services relies on third-party service providers for backup tape management, Central Services remains responsible for meeting the legal and policy obligations related to the security and protection of personal information residing on backup tapes.

Backup Tape Technology

[14] The technical specifications of backup tapes used by Central Services has evolved over time. This includes the size of tapes, algorithms used to encrypt information, and how information is written onto the tape – for example, linear sequential or diagonal. The software and hardware used to write, store and read the tapes has also evolved.

[15] Given the evolution of specifications, older tapes managed by Central Services may require the use of specialized companies that still have the means to restore and read the data on these older tapes. Engaging the services of these specialized companies can be very costly.

[16] During meetings with Central Services officials, staff indicated that there is a limit to how many times you can write and rewrite onto a backup tape. Staff indicated that consistent with standard practices, tapes are re-used. The recycling of tapes causes the tape to stretch and results in degradation over time. Staff also explained that physical deterioration of backup tapes may also be affected by environmental factors like heat and moisture if tapes are not stored appropriately. In this regard, staff indicated that manufactures of backup tapes generally provide a lifespan of approximately 70 years for tapes if they are used and stored appropriately. However, even when the appropriate measures are taken, it is still possible that a tape may be defective which could result in data being unrecoverable.

[17] Backup and recovery services do not replace records management programs that fulfill government data retention and archiving policies. These services are also not meant to serve as a preservation of information.

[18] Backup tapes need a hardware component, often referred to as a library, to read and write data. Tape libraries vary widely in technical specifications, cost and complexity. A typical library contains multiple tape drives used for reading and writing data, access ports for entering and removing tapes, scanners to read bar codes for tracking purposes, and a device for mounting and dismounting tape cartridges. A library can include hundreds of tapes.

Figure 1. Example of physical backup tapes

Figure 2. Backup tapes stored offsite by Central Services, in cases with barcodes

Figure 3. Example of a tape library

Data Stored on Backup Tapes

[19] During this investigation, Central Services confirmed that there are over 4,400 backup tapes being managed by ISM Canada and Crown Store-All on behalf of their institution. This represents a total volume of over 2.4 Petabytes of information being managed. To put this into perspective, to store one petabyte of information, it would take over 745 million floppy disks or about 1.5 million CD-ROM discs.

[20] Central Services also provided details of the specific digital information that is selected for backup purposes within each of its twenty-seven clients. Details of the specific digital information, including the specific systems backed-up, will not be provided in this report because doing so may expose this, and other government information, to security risks. Central Services, in collaboration with its clients, has selected the specific digital information that is necessary for the purposes of backup and recovery.

[21] According to Central Services staff, there is no way of knowing which backup tape contains what specific information because digital information on backup tapes is stored using binary code – which is a series of zeros and ones. As such, there is also no categorization of information or records as one would expect to exist within a records management system. Furthermore, there is nothing on the actual physical tape itself that distinguishes which backup tape contains personal information, or particularly sensitive information, unless all the data is restored.

[22] My office can safely assume, based on the list of clients of Central Services and my previous experience of conducting reviews and investigations involving these clients, that backup tapes do contain personal information and particularly sensitive information.

[23] During this investigation, my office confirmed that the Ministry of Health is not a client of Central Services for backup and storage of data. As such, Central Services does not manage backup tapes containing personal health information collected and processed by the Ministry of Health. However, during a site visit conducted by staff from my office to one

of the offsite facilities, it was discovered that backup tapes belonging to the Ministry of Health were stored in this facility. My office has contacted the Ministry of Health to advise them of this and recommended their ministry proceed with recovering their backup tapes.

[24] Digital data stored on a backup tape exists only until the next scheduled backup of information overwrites the data on that tape. The actual elapsed time between backups depends on the backup cycle and the media re-use policy for that application or system. In this regard, Central Services provided my office with information on when backups occur and how often. Such details will not be elaborated on in this report because doing so may expose the backup and recovery process to additional security risks.

[25] Information that has been "double-deleted" within a client ministry or agency before the next scheduled backup occurs is not backed up. As such, backup tapes do not represent a complete set of information and only capture data at a specific point in time.

Retention of Backup Tapes

[26] Central Services' current practice is to keep physical backup tapes indefinitely. On July 13, 2018, staff from my office met with officials from Central Services. During this meeting, officials confirmed that of the 4,400 tapes currently housed offsite, there are many backup tapes created as far back as 2004 and that contain government information from 2008 to 2010; that there is no plan to modernize these older tapes.

[27] Officials also confirmed that these tapes are at the end of their lifecycle and that Central Services has no use for these tapes, or the data residing on them. Nevertheless, Central Services continues to retain these tapes offsite along with thousands of other backup tapes.

[28] Internal and external consultations have been undertaken by Central Services' staff to discuss the retention and destruction of backup tapes and that data residing in them; however, no decision has been made yet about how long the retention period should be.

II FOCUS OF THE INVESTIGATION

[29] In Saskatchewan, government ministries and agencies create hundreds of digital records using computers every day. The type of digital records created range from generic emails to more important records used in support of the programs and services they deliver.

[30] From the thousands of digital records created everyday by the twenty-seven clients of Central Services, only a subset of the records are copied onto backup tapes. The role of Central Services is to identify the critical digital data that would need to be restored in case of a major disaster or IT system malfunction and to ensure such data is copied onto backup tapes.

[31] The focus of this investigation is therefore on the selected critical data that Central Services copies onto backup tapes and an assessment of how FOIP applies to such data. The investigation also includes how Central Services manages all backup tapes.

Out of Scope of This Investigation

[32] Digital records have introduced many challenges to proper records and information management. My office, along with other Information and Privacy Commissioners across Canada, continue to review and report on some of these challenges as it relates to compliance with access and privacy legislations.

[33] To ensure compliance with broad records management requirements in the province, ministries and agencies must implement records management programs. Ministries and agencies rely on the Provincial Archives of Saskatchewan to provide expertise and advice related to these complex programs. While there may still be challenges in how information is managed within the Government of Saskatchewan – which is also prevalent in other provinces – this investigation does not focus on the broad records and information management issues that fall under the prevue of the Provincial Archives of Saskatchewan.

[34] That being said, as the Provincial Archives of Saskatchewan provides records and information management services to the provincial government, which includes Central Services, my office provided the Provincial Archives with a copy of this report. Both the Provincial Archivist and the Director of Information Management Services support the findings and recommendations contained in this report.

[35] This investigation also does not include:

- the tapeless backup and recovery services that are being implemented in the province by Central Services;
- archiving of records to preserve information, or store it for short or long-term purposes; and
- how government ministries and agencies process access to information requests within their own institutions.

III DISCUSSION OF THE ISSUES

1. What are the relevant statutory provisions of FOIP and the FOIP Regulations applicable to this investigation?

[36] The relevant provisions of FOIP and *The Freedom of Information and Protection of Privacy Act Regulations* (FOIP Regulations) are as follows:

Subsection 2(1) defines terms used in FOIP:

> **Interpretation**
>
> **2**(1) In this Act:
>
> …
>
> (e.1) **"information management service provider"** means a person who or body that:
>
> (i) processes, stores, archives or destroys records of a government institution containing personal information; or

> (ii) provides information management or information technology services to a government institution with respect to records of the government institution containing personal information;
>
> …
>
> (g) **"personal information"** means personal information within the meaning of section 24;
>
> …
>
> (i) "**record**" means a record of information in any form and includes information that is written, photographed, recorded or stored in any manner, but does not include computer programs or other mechanisms that produce records;

Section 5 provides:

> **Right of access**
>
> **5** Subject to this Act and the regulations, every person has a right to and, on an application made in accordance with this Part, shall be permitted access to records that are in the possession or under the control of a government institution.

Subsection 5.1(1) provides:

> **Duty of government institution to assist**
>
> **5.1**(1) Subject to this Act and the regulations, a government institution shall respond to a written request for access openly, accurately and completely.

Section 24.1 provides:

> **Duty of government institution to protect**
>
> **24.1** Subject to the regulations, a government institution shall establish policies and procedures to maintain administrative, technical and physical safeguards that:
>
> > (a) protect the integrity, accuracy and confidentiality of the personal information in its possession or under its control;

(b) protect against any reasonably anticipated:

(i) threat or hazard to the security or integrity of the personal information in its possession or under its control;

(ii) loss of the personal information in its possession or under its control;
Or

(iii) unauthorized access to or use, disclosure or modification of the personal information in its possession or under its control; and

(c) otherwise ensure compliance with this Act by its employees.

Section 24.2 provides:

Information management service provider

24.2(1) A government institution may provide personal information to an information management service provider for the purposes of:

(a) having the information management service provider process, store, archive or destroy the personal information for the government institution;

(b) enabling the information management service provider to provide the government institution with information management or information technology services;

(c) having the information management service provider take possession or control of the personal information;

(d) combining records containing personal information; or

(e) providing consulting services.

(2) Before disclosing personal information to an information management Service provider, a government institution shall enter into a written agreement with the information management service provider that:

(a) governs the access to and use, disclosure, storage, archiving, modification and destruction of the personal information;

(b) provides for the protection of the personal information; and

(c) meets the requirements of this Act and the regulations.

(3) An information management service provider shall not obtain access to, use, disclose, process, store, archive, modify or destroy personal information received from a government institution except for the purposes set out in subsection (1).

(4) An information management service provider shall comply with the terms and conditions of the agreement entered into pursuant to subsection (2).

Subsections 6(1), 7(1) and 7(2) of the FOIP Regulations provide:

Fees

6(1) Where access to a record or part of a record is given by providing the applicant with a copy of the record, the following fees are payable at the time when access is given:

(a) for a photocopy, $0.25 per page;

(b) for a computer printout, $0.25 per page;

(b.1) for electronic copies, the actual cost of the portable storage device provided to the applicant;
…

(l) for a form of record not mentioned in clauses (a) to (b.1), the actual cost of copying the record.

Estimate

7(1) For the purposes of subsection 9(2) of the Act, $100 is prescribed as the amount of fees beyond which an estimate must be given by the head.

(2) Where the amount of an estimate exceeds the actual amount of fees determined pursuant to section 6, the actual amount of fees is the amount payable by the applicant.

Section 13.1 of the FOIP Regulations provide:

Agreement between government institution and information management service provider

13.1 For the purposes of clause 24.2(2)(c) of the Act, a written agreement

> that is entered into between a government institution and an information management service provider must include:
>
> > (a) a description of the specific service the information management service provider will deliver;
> >
> > (b) provisions setting out the obligations of the information management service provider respecting the security and safeguarding of personal information; and
> >
> > (c) provisions for the destruction of the personal information, if applicable.

2. How do the relevant provisions of FOIP and FOIP Regulations apply to data stored on backup tapes?

Is data stored on a backup tape the "primary record" within the meaning of subsection 2(1)(i) of FOIP?

[37] One of the purposes of FOIP is to provide individuals with a right of access to records within government institutions. As stated in my office's guide, *Best Practices for Responding to Access Requests*, available online at https://oipc.sk.ca/assets/best-practices-for-responding-to-access-requests.pdf, for the purposes of FOIP, a record is the package of documents that would be responsive to an individual's access request and that are in the possession or control of the government institution. The access provisions of FOIP are "record-driven" and not "information-driven."

[38] In the context of FOIP, "possession" means physical possession, plus a measure of control of the record. "Control" connotes authority. A record is under the control of a government institution when the institution has the authority to manage the record including restricting, regulating and administering the records use, disclosure or disposition.

[39] When an individual makes an application for access to records, ministries and agencies should be providing the package of documents that would be responsive to the individual's request, and the documents in their possession or control.

[40] As described in the Background section of this report, backup tapes managed by Central Services contain only copies of uncategorized and critical digital data that already exists elsewhere within one of the twenty-seven clients of Central Services. The original copy of the data should be appropriately stored and retained in accordance with existing legal and policy requirements related to the management of records within the Government of Saskatchewan. If appropriate records management practices exist, then any one of the twenty-seven clients of Central Services who receives an application for access to records under FOIP should be able to conduct a reasonable search for responsive records, regardless of what may or may not exist on backup tapes managed by Central Services.

[41] The sole purpose of copying digital data that already exists elsewhere onto a backup tape is to allow Central Services to restore the data in case of a major disaster or IT system malfunction. Data resides on a tape for the specified and limited period of time that it is needed to serve its purpose. This means that every time Central Services creates a new backup of data for one of its clients, the previous backup is no longer needed and ceases to serve any purpose. This continuous creation of backups does not alter, modify, nor affect the original copy of the data in any way.

[42] In 2009, Nova Scotia's Freedom of Information and Protection of Privacy office issued a report (FI-08-26(M)) where the Review Officer noted that:

> …Back-up tapes are for recovery purposes only and at this time are not considered a primary record. Back-up systems are designed to re-establish entire systems in the event of a systems catastrophe and are not set up or intended to be a means of retrieving individual emails. The British Columbia Commissioner agrees with that analysis regarding back-up emails…

[43] The British Columbia (BC) Commissioner's analysis referred to in the 2009 Nova Scotia report may be found in his report Order 02-25, which states:

> A separate issue under s. 6(1) is whether the Ministry was required to restore deleted e-mails in responding to the applicant's request. Relying on several of my predecessor's decisions on this point, the Ministry says s. 6(1) duty does not require

> it to find and restore to intelligible form e-mails that have been deleted and exist only in back-up tapes. See, for example, Order No. 73-1995, [1995] B.C.I.P.C.D. No. 46, and Order No. 198-1997, [1997] B.C.I.P.C.D. No. 59.
>
> The Ministry says back-up systems are designed to re-establish entire e-mail systems in the event of a catastrophe, not for retrieving individual deleted e-mails. Section 6(1) requires public bodies to make reasonable efforts to retrieve records and retrieving deleted e-mail messages from backup tapes exceeds a reasonable effort, the Ministry argues. Moreover, it says, there is no reason to believe there are any responsive deleted e-mails and it would be a complex, costly and time-consuming exercise to recover and search back-up tapes to determine if any such records exist (paras. 4.07-4.13, initial submission).
>
> I agree with the Ministry that, in these circumstances, its s. 6(1) duty does not extend to retrieving deleted e-mail messages.

[44] In its findings, the Nova Scotia Review Officer stated that "The Applicant is not entitled to any back-up emails, save and except for any emails that were on the current system when the [application] was received and were deleted and are on back-up". In its conclusions, the BC Commissioner stated that the Ministry had complied with its duty to respond to the applicant openly, accurately and completely in its search for records, even when it had not searched for deleted e-mail messages on backup tapes. This position of the BC Commissioner's was reiterated in a more recent report, Order F19-04.

[45] I agree with the analysis and findings of the Nova Scotia Review Officer and the British Columbia Commissioner. I would add that, in regards to possession or control of records, it is reasonable to accept that Central Services, not its clients, is in possession and control of the data stored on backup tapes. This is because Central Services plays the principal role in:

- creating the copies of data stored on backup tapes;
- establishing when backups are created and how;
- using backups in case of a disaster for recovery purposes; and
- overseeing the overall management of backup tapes and the data on those tapes.

[46] In light of the above, I find that the data that resides on backup tapes is not the "primary record" that falls within the meaning of subsection 2(1)(i) of FOIP; I find that this data is merely a copy of the data that already exists elsewhere, and it serves a completely different

purpose. Accordingly, the data that already exists elsewhere, the original copy of the data, is in fact the "primary record" that would be responsive to an application for access to records under FOIP.

Is there a requirement to search through data stored on backup tapes in response to a request for access?

[47] Since data stored on backup tapes is not the "primary record" that falls within the meaning of subsection 2(1)(i) of FOIP, I find that backup tapes do not need to be included in a search for responsive records when processing an application under FOIP. FOIP imposes on government institutions a duty to assist requirement that in part requires institutions to make every reasonable effort to identify and seek out responsive records. However searching within backup tapes exceeds the reasonable efforts required by the duty to assist requirement, as was also noted in the BC Commissioner's Order 02-25 and F19-04.

[48] For years, Central Services has been offering its clients a service whereby they provide assistance with searching in backup tapes for responsive records. On June 27, 2018, staff from my office met with the Service Manager at Central Services who is responsible for overseeing the search requests received from Central Services' clients.

[49] The Service Manager confirmed that the requests from clients are almost all related to email accounts that are no longer active. These email accounts are not active either because an employee has left the ministry or agency and the account was deleted, or an employee is on extended leave and the account is inaccessible. If the request involves an inactive email account prior to 2010, Central Services relies on the backup tapes to search for the email account requested by its client. Central Services has created procedures to outline how Central Services processes a search request from one of its clients.

[50] On July 13, 2018, officials from Central Services reiterated that in their view, inadequate records management practices, including the lack of a mandatory centralized document repository, may be their clients' greatest challenge as it pertains to records management and storage. Because of this, Central Services indicated that many clients rely on their

institution to search through data stored on backup tapes to retrieve responsive records when processing an application for access to records under FOIP.

[51] While I commend Central Services for the time and resources their institution has dedicated to offering the search-related service to its clients, searches within backup tapes have raised a number of other issues as it relates to the FOIP requirements. For instance, inappropriate search-related fee estimates have been provided to applicants, as noted in a November 2017 news article, which reported that a government ministry sought to charge an applicant $96, 000 to search through backup tapes. In another case, my office's Review Report 078-2016 to 091-2016 found that a $100,160 fee estimate given to an applicant was inappropriate because the government institution did not have appropriate records management practices in place and needed the assistance of Central Services to search for responsive records.

[52] Not only can searching within backup tapes be costly and potentially discourage the exercise of rights under FOIP, but in a recent case, Investigation Report 262-2017, my office was prevented from conducting a full investigation and reviewing relevant records. The institution involved in this case advised my office that they believed Central Services was keeping their official records on backup tapes, so they did not appropriately retain and store official records within their own institution. The institution involved also advised my office that after consulting with Central Services, retrieving the records from backup tapes was too costly and time-consuming; therefore, they were unable to provide my office with the pertinent records. This is a problem and it is unacceptable.

[53] In light of the above, and because backup tapes do not need to be included in a search for responsive records when processing an application under FOIP, I recommend Central Services immediately stop offering the search-related service to its clients, where an application for access to records under FOIP is concerned. I also recommend that Central Services inform its clients that it will cease to offer this service and use this opportunity to clarify the purpose of backup and recovery services to avoid any confusion about what Central Services is copying onto backup tapes and why.

[54] Once Central Services ceases to offer their search-related service, more of the records management issues within government institutions may become evident as part of my office's reviews and investigations pursuant to FOIP. In this respect, my office will take the opportunity to discuss these issues in future reports.

Are there Exceptions to Searching within Backup Tapes?

[55] I find that there may be exceptions to when it may be appropriate for Central Services to assist an institution with searching for records, as it relates to the FOIP requirements. For example, if an institution receives an application for access to records under FOIP and an officer within that institution either knowingly or accidentally deletes responsive records, it is possible that the only copy of responsive records exists within backup tapes. This exception was also noted in the Nova Scotia Review Officer's report, FI-08-26(M). In these cases, applicants should not be expected to cover the expensive costs associated with searching for, and retrieving, records from backup tapes.

[56] I recommend that Central Services implement written procedures to outline under what exceptional circumstances their institution may search within backup tapes as it relates to the FOIP requirements, and I recommend Central Services share these procedures with its clients.

How long do backups and backup tapes need to be retained as per FOIP?

[57] During this investigation, staff from Central Services informed my office that they have concerns over destroying backup tapes that no longer serve any purpose and that are at the end of their lifecycle because they may contain the only copy of a client's records. Central Services explained that this is contributing to the indefinite retention of tapes and the retention of thousands of backup tapes offsite.

[58] *The Ministry of Central Services Regulations, 2016*, permits Central Services to develop, promote and implement policies and programs of the Government of Saskatchewan

relating to information technology, information management and records management. This allows Central Services to offer backup and recovery services and develop and implement the framework needed to support those services.

[59] Frameworks in support of programs and services of an institution should cover off the information management lifecycle of all information and records created, used, stored, destroyed and preserved as part of the program or service. It is unclear why Central Services could implement a framework for backup and recovery services, but not proceed with establishing the necessary retention and destruction of backups and backup tapes.

[60] The Administrative Records Management System (ARMS), developed by the Provincial Archives of Saskatchewan under the authority of *The Archives and Public Records Management Act*, applies to all Saskatchewan government ministries, including Central Services. ARMS combines a classification system and records retention schedules. The retention schedules indicate the minimum time a government institution must retain an official record and serves as a legal tool for disposing of the record once its retention period is met and its usefulness is complete. ARMS contains a retention schedule, TR60 System Backup Files, related to backup files:

> **TR60 System Backup Files**
>
> Files routinely made for security of information and emergency system recovery purposes.
>
> Note: System backup files are only required for limited periods of time in order to meet the administrative and operational requirements of government agencies. System backups are typically made on a daily, weekly, monthly and/or annual basis.
>
> Backups usually include data or data extractions, but may also include commercial or custom-designed software. Backup procedures and their frequency may differ from system to system. An acceptable practice is to re-use electronic backup media according to a re-use schedule established on a system-by-system basis.
>
> This classification does not apply to disk or tape backups made for other purposes. For example, electronic records transferred to tape, disk, etc., for long

> term preservation must be classified by functions, and disposed according to an approved records schedule.
>
> Retention: Disposal of these records through destruction or re-use of the media may proceed according to internal disposal procedures.

[61] The above noted retention schedule states that institutions are to develop internal disposal procedures regarding the retention of backups. This provides Central Services with the flexibility of establishing the necessary retention period their institution deems necessary for backups to fulfil their purpose.

[62] I have already found in the preceding sections that data stored on backup tapes is not the "primary record" within the meaning of FOIP, and that backup tapes do not need to be included in a search for responsive records when processing an application for access to records under FOIP – aside from any exceptional cases that may exist. As such, I find that there is no FOIP requirement that prevents Central Services from destroying the information on a backup tape, or the backup tapes themselves, as long as the institution complies with the legal and policy requirements related to the retention and destruction of this type of data under *The Archives and Public Records Management Act*.

[63] I recommend that Central Services establish an internal retention and disposal procedure for backups and backup tapes within one year of issuance of this report. This procedure should specify how long backups and backup tapes are to be retained and whether backup tapes will be re-used. In addition, the procedure should specify when and how tapes will be securely destroyed. Once the internal procedure is developed, I recommend Central Services append this internal procedure to its third-party service provider's contract and to the Service Level Agreements with its clients.

Is data stored on backup tapes subject to protections in accordance with FOIP?

[64] As of January 1, 2018, section 24.1 of FOIP came into force and it imposes an obligation on government institutions to protect personal information in its possession or under its

control. Though section 24.1 is a new amendment to FOIP, my office has always expected institutions, subject to FOIP, to protect personal information in their possession or control.

[65] Section 24.1 requires that institutions establish policies and procedures to maintain administrative, technical, and physical safeguards that protect the integrity, accuracy and confidentiality of personal information. It also requires that institutions maintain policies and procedures to protect against any reasonably anticipated threat or hazard to the security, integrity, loss, unauthorized access to or use, disclosure or modification of personal information.

[66] Maintaining safeguards requires that safeguards continue to be appropriate and work as intended. With this in mind, my office expects that policies implemented in accordance with section 24.1 of FOIP should require that Threat and Risk Assessments (TRAs) and Privacy Impact Assessments (PIAs) be undertaken before programs and services that involve personal information are implemented. TRAs and PIAs have been in use for many years and assist institutions in identifying reasonable privacy and security threats or hazards to information, so that appropriate safeguards – administrative, technical or physical safeguards – are implemented. While these assessments are often conducted separately because their scope and purpose is different, it is a best practice to combine the findings and recommendations from these assessments for efficiency purposes as findings from one assessment can serve as inputs into the other assessment, and vice versa. Although these assessments should be done before programs and services are implemented to be most effective, they can also be valuable after implementation.

[67] TRAs and PIAs are meant to identify threats or hazards at a specific point in time; therefore, it is necessary to review and update these assessments regularly, as a common best practice. This continuous assessment of privacy and security threats or hazards to information allows institutions to maintain administrative, technical and physical safeguards that protect personal information, and in my view would serve to meet, in part, the requirements of section 24.1 of FOIP.

[68] In addition to implementing policies requiring the use of TRAs and PIAs, my office also expects government institutions to implement policies and procedures that practically outline how the institution will comply with the requirements of PART IV Protection of Privacy pursuant to FOIP. This includes specific policies and procedures related to the collection, accuracy, use, disclosure, access and right of correction of personal information, among other requirements. Policies and procedures related to training and awareness of privacy requirements, privacy breaches and complaint mechanisms are also other documents my office expects institutions to implement to comply with section 24.1 of FOIP.

[69] While my office did not verify the specific contents of the backup tapes, I can safely assume based on the list of Central Services' clients and my office's previous experience in conducting reviews and investigations involving these clients, that tapes do contain personal information as defined in subsection 24(1) of FOIP. Even if the data on backup tapes is stored in binary code and in an uncategorized way, the tapes nevertheless contain personal information about identifiable individuals. Since Central Services is unable to distinguish between the backup tapes that contain personal information and those that do not, I find that Central Services has a duty to protect all backup tapes in accordance with section 24.1 of FOIP.

[70] During this investigation, my office did not assess whether Central Services had the required policies and procedures in place to comply with section 24.1 of FOIP. However, staff from my office visited two of the offsite storage locations and made general inquiries with Central Services about the administrative, technical and physical safeguards in place at these locations. Additionally, my office inquired whether physical TRAs had been undertaken.

[71] Generally, my office found there to be adequate controls at the offsite storage locations, though there were a few areas that could be improved. For instance, there is no process in place between all parties – Central Services, the third-party service provider ISM and the

subcontractor – for how security and privacy incidents will be managed should a backup tape be misplaced, lost or stolen.

[72] Additionally, my office noted that there was insufficient segregation of backup tapes belonging to Central Services and those belonging to other organizations. At one location, all backup tapes were kept in the same general, protected area. In another location, tapes were stored on open shelves among other tapes belonging to other clients of the subcontractor. Given that an inventory of the Central Services backup tapes is only done once a year, it could take a long time for Central Services, or ISM, to identify if a backup tape has been misplaced, lost or stolen. Moreover, my office found some tapes stored in boxes with security tape that was already broken and significantly degraded. Security tape is often used to identify when boxes have been accessed by looking at whether the tape is intact or not. Unfortunately, in this case security tape was not being used appropriately.

Figure 4. Pictures taken at offsite storage facility that show backup tapes on open shelves and the degraded security tape in use.

[73] In terms of physical access controls, my office found that only one location had advanced access controls. This is concerning given the importance of the data on backup tapes and the type of information, even if encrypted, that resides on those tapes. Central Services confirmed that no physical TRAs have been completed at either of the locations visited. However, they confirmed that security audits have been conducted in the past and provided my office with copies of documents containing the results of these audits. Despite previous security audits, I find that there are areas regarding the management of backup tapes that

need improvement in order for Central Services to comply with its obligations to protect personal information pursuant to section 24.1 of FOIP.

[74] Within one year of issuance of this report, I recommend that Central Services conduct physical TRAs for all offsite locations where backup tapes are stored and ensure that TRAs address the areas identified in this report. I also recommend that Central Services assess whether PIAs should be undertaken to complement the TRAs to be completed. Finally, I recommend that Central Services review its policies and procedures related to the management of backup tapes to ensure these documents are in line with my office's expectations as it relates to section 24.1 of FOIP.

[75] During this investigation, Central Services advised my office that there are approximately 3,000 tapes that are under a litigation hold because of an ongoing Government of Saskatchewan litigation. As such, although the tapes are no longer needed by Central Services – for any administrative or operational requirement or purpose related to backup and recovery services – the tapes must continue to be retained for the purpose of litigation.

[76] Within one year of issuance of this report, I recommend that Central Services develop a plan for how they will manage these 3,000 tapes, and any new tapes that may be created, that fall under the litigation hold. The plan should indicate:

- the scope of the litigation hold and details of the backup tapes that are subject to the litigation hold;
- whether Central Services will continue to retain custody and control of backup tapes, or transfer custody and control to another government ministry;
- how the overall management of the backup tapes subject to the litigation hold will be managed, taking into consideration the comments and recommendations in this report regarding safeguards and third-party information management service providers; and
- the retention schedule that applies to the tapes.

[77] If in the process of developing their plan, Central Services identifies any tapes that do not fall under the litigation hold and that are no longer needed for any administrative requirement or purpose, and that are at the end of their lifecycle, these tapes should be destroyed; any destruction of tapes should comply with government security policies. Once the plan has been developed and approved, Central Services should provide a copy to my office.

Are there FOIP requirements that apply to the third-party service providers who manage backup tapes on behalf of Central Services?

[78] Central Services relies on a third-party service provider, ISM, and a subcontractor for the day-to-day management of backup tapes. As of January 1, 2018, section 24.2 of FOIP and section 13.1 of the FOIP Regulations came into force which requires that institutions who provide access to personal information to a third party and who rely on a third party to store personal information must have a written agreement in place with that third party. The written agreement must outline:

- the specific service(s) the information management service provider will deliver;
- how access, use, disclosure, and storage of personal information will be carried out by the third party;
- specify the obligations of the information management service provider respecting the security and safeguarding of personal information. For example by requiring the third party to conduct threat and risk assessments and privacy impact assessments;
- specify how the third party, acting on behalf of an institution, will meet the requirements of FOIP;
- state the consequences for not complying with the terms and conditions of the agreement;
- include audit provisions that allow an institution to verify that the third party is complying with the agreement; and

- specify how often the agreement will be reviewed to ensure continued compliance with any legal and policy obligations, including any amendments to FOIP and the regulations that may come into force in the future.

[79] Since backup tapes contain personal information, and an information service provider as defined in FOIP manages this information, I find that the requirements of section 24.2 of FOIP apply to the management of backup tapes and the data residing on those tapes.

[80] Central Services has a contract in place with ISM but Central Services confirmed that this contract has not been reviewed since the new requirements to FOIP and the FOIP Regulations came into force. Central Services also confirmed that ISM and the subcontractor have a contract in place, but there is no Statement of Work that defines the specific activities to be undertaken by the subcontractor. Central Services indicated that the processing and tape movement procedures between ISM and the subcontractor are defined outside of the contract and managed internally.

[81] I recommend that Central Services review the existing contract with ISM to ensure it complies with section 24.2 of FOIP. Additionally, I recommend that Central Services require that ISM and the subcontractor have a written agreement in place that is also compliant with section 24.2 of FOIP. As a government institution subject to FOIP, Central Services must ensure that any third party providing IT services or carrying out activities on their institution's behalf, including any subcontractor, also complies with FOIP.

III FINDINGS

[82] I find that the data that resides on backup tapes is not the "primary record" that falls within the meaning of subsection 2(1)(i) of FOIP; I find that this data is merely a copy of the data that already exists elsewhere, and it serves a completely different purpose.

[83] I find that backup tapes do not need to be included in a search for responsive records when processing an application under FOIP.

[84] I find that there may be exceptions to when it may be appropriate for Central Services to assist an institution with searching for records, as it relates to the FOIP requirements.

[85] I find that there is no FOIP requirement that prevents Central Services from destroying the information on a backup tape, or the backup tapes themselves, as long as the institution complies with the legal and policy requirements related to the retention and destruction of this type of data under *The Archives and Public Records Management Act*.

[86] I find that until backup tapes are destroyed in accordance with a retention schedule, Central Services has a duty to protect all backup tapes in accordance with section 24.1 of FOIP.

[87] I find that there are areas regarding the management of backup tapes that need improvement in order for Central Services to comply with its obligations to protect personal information pursuant to section 24.1 of FOIP.

[88] I find that the requirements of section 24.2 of FOIP apply to the management of backup tapes and the data residing on those tapes.

IV RECOMMENDATIONS

[89] I recommend Central Services immediately stop offering the search-related service to its clients, where an application for access to records under FOIP is concerned.

[90] I recommend that Central Services inform its clients that it will cease to offer the search-related service and use this opportunity to clarify the purpose of backup and recovery services to avoid any confusion about what Central Services is copying onto backup tapes and why.

[91] I recommend that Central Services implement written procedures to outline under what exceptional circumstances their institution may search within backup tapes as it relates to

the FOIP requirements, and I recommend Central Services share these procedures with its clients.

[92] I recommend that Central Services establish an internal retention and disposal procedure for backups and backup tapes within one year of issuance of this report.

[93] Once the procedure recommended above is developed, I recommend Central Services append this procedure to its third-party service provider's contract and to the Service Level Agreements with its clients.

[94] Within one year of issuance of this report, I recommend that Central Services conduct physical TRAs for all offsite locations where backup tapes are stored and ensure that TRAs address the areas identified in this report where improvements are needed.

[95] I recommend that Central Services assess whether PIAs should be undertaken to complement the TRAs to be completed.

[96] Within one year of issuance of this report, I recommend that Central Services develop a plan for how they will manage the 3,000 tapes, and any new tapes that may be created, that fall under the ongoing litigation hold.

[97] I recommend that Central Services review its policies and procedures related to the management of backup tapes to ensure these documents are in line with my office's expectations as it relates to section 24.1 of FOIP.

[98] I recommend that Central Services review the existing contract with ISM to ensure it complies with section 24.2 of FOIP.

[99] I recommend that Central Services require that ISM and the subcontractor have a written agreement in place that is also compliant with section 24.2 of FOIP and 13.1 of the FOIP Regulations.

Dated at Regina, in the Province of Saskatchewan, this 8th day of March, 2019.

Ronald J. Kruzeniski, Q.C.
Saskatchewan Information and Privacy Commissioner

Annex A – List of Central Services Clients for Backup and Recovery Services

	Name of Ministry or Agency
1.	SaskBuilds
2.	Physician Recruitment Agency of Saskatchewan
3.	Highways and Infrastructure
4.	Government Relations
5.	Global Transportation Hub Authority
6.	Education
7.	Central Services - Wascana
8.	Central Services - Government House
9.	Central Services
10	Agriculture
11	Trade and Export Development
12	Sask Municipal Board
13	Public Service Commission
14	Labour Relations and Workplace Safety
15	Immigration and Career Training
16	Finance
17	Executive Council and Office of the Premier
18	Energy and Resources
19	ATCC
20	Advanced Education
21	Social Services
22	Sask Housing Corporation
23	Parks, Culture, & Sport
24	Justice and Attorney General
25	Correction and Policing
26	Financial and Consumer Affairs Authority
27	Environment