**ᓄᓇᕗᒻᒥ ᑐᓴᐅᒪᔪᓕᕆᓂᕐᒧᑦ ᑲᓐᓄᓇᖅᑐᓕᕆᓂᕐᒧᓪᓗ ᑲᒥᓯᓇ**
**Nunavut Information and Privacy Commissioner**
**Nunavunmi Tuhaqtauyukhaliqinirmun Kanngunaqtuliqinirmun Kamisina**
**Commissaire à l’information et à la protection de la vie privée du Nunavut**

# Commissioner’s Special Report

| | |
|---|---|
| **Report Number:** | 23-245-SR |
| **CanLII Citation:** | Department of Executive and Intergovernmental Affairs and twelve other public bodies (Re), 2023 NUIPC 12 |
| **NUIPC File Number:** | 22-127 |
| **Date:** | June 1, 2023 |

## Summary

**[1]** The Commissioner initiated a review of the GN network drive known as the Y-drive. The Commissioner asked thirteen public bodies to self-audit their Y-drive to assess the risk of privacy breaches. All thirteen carried out the self-audit and reported to the Commissioner. The Commissioner finds that the Y-drive does not meet the “reasonable security arrangements” standard in section 42 of the ATIPPA, and makes certain recommendations to reduce the risk of privacy breaches on the Y-drive.

## Nature of Review and Jurisdiction

**[2]** This is a special report. I initiated the review under section 49.1(2) of the *Access to information and Protection of Privacy Act* (ATIPPA). The purpose of the review was to assess the privacy practices of GN public bodies with respect to the computer network drive commonly referred to as “the Y-drive”.

**[3]** I have jurisdiction over all departments of the GN and over the public bodies listed in Schedule A of the ATIPP Regulations. This jurisdiction is broad enough to cover all departments and public bodies that use the Y-drive.

## Background to the Review

**[4]** In the fall of 2021, I received information that there was a privacy problem with a GN computer network drive commonly referred to as "the V-drive". The V-drive was used to share files between GN departments with offices in the same community.

**[5]** My review found a large number of privacy-invasive records on the V-drive that could be seen by anyone with V-drive access in the same community. The Department of Community and Government Services (CGS), which has overall responsibility for the GN's computer network, worked with me and the Territorial ATIPP Manager to remove the most obviously privacy-invasive files. CGS eventually decommissioned the V-drive entirely, and replaced it with a different, more secure method of sharing files.

**[6]** My report on the V-drive was published as *Department of Community and Government Services (Re)*, 2022 NUIPC 2 (CanLII). It is also available on the NUIPC website (atipp-nu.ca) as Review Report 22-211.

**[7]** As a result of publicity around my V-drive report, I received information from some GN employees that the Y-drive was also a privacy risk. (One quotation: "If you think the V-drive was a problem, you should see the Y-drive.") The Y-drive is used to share files within a department in the same community.

**[8]** To evaluate the seriousness of the Y-drive privacy risk, I test-audited the Iqaluit Y-drive of the Department of Family Services (DFS). The results of the test audit were worrisome. There was a great deal of personal information on the Y-drive, some of it highly sensitive, that could be viewed by departmental employees who had no operational need to see it. There was no organization to the filing system and nobody was responsible for the organization or security of the files. There was therefore an enhanced risk that personal information would be forgotten, misplaced, or inappropriately accessed.

**[9]** Based on this test audit, I concluded that the Y-drive probably represented a substantial privacy risk at every public body that used it.

**[10]** On June 3, 2022, I wrote to all eleven departments and the two public agencies that use the Y-drive. Those public bodies, and the abbreviations I use for them in the rest of this report, are:

a. Department of Community and Government Services (CGS)
b. Department of Culture and Heritage (CH)
c. Department of Economic Development and Transportation (EDT)
d. Department of Education (EDU)
e. Department of Executive and Intergovernmental Affairs (EIA)
f. Department of Environment (ENV)
g. Department of Finance (FIN)
h. Department of Family Services (DFS)
i. Department of Health (HEA)
j. Department of Human Resources (HR)
k. Department of Justice (JUS)
l. Nunavut Arctic College (NAC)
m. Nunavut Housing Corporation (NHC)

In the letter, I outlined my concerns. I asked each public body to undertake a self-audit of their Y-drive. I asked them to report back to me no later than December 1, 2022. On October 24, 2022, I sent a reminder letter.

**[11]** As I explained in my letters of June 3, 2022, I do not have the legal authority to <u>compel</u> a public body to undertake a self-audit of their Y-drive. I can only <u>ask</u>, and if there is a refusal, bring the refusal to the attention of the Legislative Assembly.

**[12]** By December 1, 2022, or within a few days thereafter, I received reports from all public bodies to which I had written, except CH and NHC. CH submitted preliminary findings on December 2, but needed more time to complete its self-audit. I received CH's final report on February 7, 2023. NHC had started its self-audit before December 1, but for a variety of reasons was unable to finish by the deadline. After discussion, NHC and I agreed that their report would be submitted no later than the end of March 2023. I received NHC's report on March 28, 2023.

**[13]** On April 11, 2023, I circulated a draft of this report to all thirteen public bodies, and asked for any comments on the draft to be provided to me no later than May 15, 2023. I received none.

## Legal framework

**[14]** Section 42 of the ATIPPA lays down the standard for protection of personal information within the GN:

> The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

**[15]** The standard laid down in section 42 – "reasonable security arrangements" – is vague. It has to be supplemented by policies, procedures, best practices, and vigilance. My recent decision in *Department of Health (Re)*, 2023 NUIPC 6 (CanLII) at paragraph 49, fills in some of the details of what "reasonable security arrangements" look like. I will not repeat that analysis here, but I adopt it for purposes of this report.

**[16]** There are certain other laws that stipulate the standard for data protection. The *Adoption Act*, for example, lays down strict rules about the protection of adoption information. I asked each public body to identify any legislation within their area of responsibility that lays down a special rule about data protection. A few had some special statutory rules to follow (e.g. HEA, JUS) but most did not.

## Description of the Y-drive

**[17]** Until recently, CGS maintained three network drives for digital file storage:

a. The V-drive was available to GN users within a community. This allowed for file sharing between departments within a community. (As noted above, the V-drive has been decommissioned.)

b. The Y-drive is available to GN users within a community and within the same department.

c. The U-drive is available to GN users for their own files. This allows a user to access files from any GN computer to which they sign on, while eliminating the need to store files on a device.

**[18]** CGS's Information Management/Information Technology (IM/IT) division manages the technical side of the drives through their system administrators. CGS operates the Y-drives for most entities within the GN, including all departments and NAC. NHC has a Y-drive and also its own shared drive.

**[19]** The Y-drive is not one drive, but rather a series of network drives. If a department is present in all 25 communities plus Ottawa, it has 26 Y-drives. A few public bodies, such as Health, are present in every community. Some are present in a subset of communities – EIA, for example, has a Y-drive in 12 communities. Typically the public body's largest Y-drive is in Iqaluit. In some communities, a department may have a Y-drive but departmental staff do not use it.

**[20]** Throughout this report I use the term "Y-drive" in the singular, but it should be understood, except where the context indicates otherwise, as a reference to all of a public body's Y-drives.

**[21]** In technical terms, each Y-drive is a mapped network drive. It is a virtual storage area that allows users to access folders and files stored on network servers. The Y-drive is an approved GN records depository. Departments use their Y-drive to store and access departmental records.

**[22]** Each Y-drive has security properties. These properties can be modified by system administrators. Each drive, and the folders on the drive, and the files within the folders, have "permissions" that govern who can view, edit, modify, and move them. Permissions can be given to individuals or groups of individuals ("user groups").

**[23]** In non-technical terms, the Y-drive is like a giant information warehouse. The warehouse is divided into individual rooms, one for each public body, and further divided into smaller rooms, one for each community in which the public body is active. CGS looks after the warehouse as a whole and assigns rooms to each public body. As for what goes on inside those rooms, that is up to each public body – and that is where the problem lies.

### Purpose and Methodology of the Review

**[24]** When I wrote to the thirteen public bodies on June 3, 2022, I left it up to each public body to determine how best to carry out the self-audit.

**[25]** The primary goal of the self-audit was to get each public body to contemplate, in a sustained and organized way, the privacy risks inherent in its Y-drive. That primary goal was achieved when the thirteen public bodies finished their self-audits and submitted their reports to me.

**[26]** I did not ask for, and I did not expect, a "forensic" audit – an audit in which every file and every document is examined. Most of the Y-drives have far too many files and documents for that. FIN, for example, has more than 2.1 million documents in 226,605 folders. Even a small department like CH has 87,974 folders and sub-folders. What I did expect was that each public body would take a systematic look at their Y-drives, and assess where the greatest privacy risks were.

**[27]** I also did not ask that each public body, as part of the self-audit, actually clean up its Y-drive. Now that the self-audits have been done, I expect each public body will want to clean up quickly the most problematic and privacy-invasive portions of their Y-drives. Some have already done so. Once that is done, their follow-up to non-urgent issues is an operational decision best left to each public body, to be balanced against other issues and priorities.

**[28]** The Territorial ATIPP Manager took the lead on developing an audit tool. I understand he received substantial assistance from Shawn Morrissey and the Records Management team in CGS; Karim Metali, Senior Database Administrator in the IM/IT division of CGS; and Jessica Waldinger, ATIPP Coordinator at EDT. I acknowledge their efforts.

**[29]** The audit tool was intended to guide the public body through the Y-drive in each community and perform a triage of privacy risk: high risk, medium risk, and low risk.

**[30]** Most public bodies applied the audit tool, though with varying degrees of rigour. The most rigour appears to have been applied by EIA itself, along with FIN. The results at those two public bodies are detailed and clear. The results at other public bodies lie along a spectrum of less detail and less clarity. Some public bodies, notably HEA, developed and applied their own audit methodology.

**[31]** All thirteen public bodies submitted a report with their audit results. Most public bodies, with the exception of EDT and DFS, submitted a report directly to me. EDT and DFS submitted their report to the Territorial ATIPP Manager. The Territorial ATIPP Manager submitted a report for EIA (his home department) and a summary report for all other public bodies including EDT and DFS.

**[32]** I am satisfied with the effort made by each public body to perform the self-audit and report the results.

### Criteria for evaluation

**[33]** A privacy-protective Y-drive should exhibit at least the following features:

a. Responsibility: The public body should take responsibility for the organization of its Y-drive, and within each public body there should be an identifiable person who is accountable for management of personal information on the Y-drive.

b. Privacy by design: Technological design of the Y-drive should support the protection of personal information. Default settings should be privacy-protective.

c. Contextual protection: The degree of privacy protection should be commensurate with the context. The more sensitive the personal information, the greater the protection it needs.

d. Logical organization: The Y-drive should be organized in a standard, logical, user-friendly way.

e. Need to know: Files on the Y-drive containing personal information should be accessible only by those employees who need to see them to do their jobs.

f. Least disclosure: When an employee needs to see personal information on the Y-drive, they should be able to see only the amount necessary for them to do their jobs.

g. Full life-cycle protection: Personal information on the Y-drive should be protected through its full life-cycle, from the time the personal information is placed on the Y-drive, up to and including its planned destruction or archiving.

h. Documentation: There should be written policies and procedures for the Y-drive. These policies and procedures should be readily available to staff using the Y-drive.

i. Audit trail: When there is a question about who viewed personal information on the Y-drive, an audit trail should be available.

**Application of the criteria to the reports**

*a. Responsibility*

**[34]** The public body should take responsibility for the organization of its Y-drive, and within each public body there should be an identifiable person who is accountable for management of personal information on the Y-drive.

**[35]** The self-audits show that most public bodies had not, prior to the audit, given much thought to their Y-drive. It was there. Their employees used it.

**[36]** FIN noted that a former senior manager had kept the department's Y-drive well-organized. That work was admirable, and helped to ensure that FIN's Y-drive is among the best-organized in the GN. But it was personal project of the manager, and it lasted only as long as that manager was in the position.

**[37]** In response to my question about whether anyone within the public body has responsibility for privacy, most public bodies named their ATIPP Coordinator.

In my view, the ATIPP Coordinators are not, for the most part, well-positioned to have overall responsibility for privacy.

**[38]** I think it would surprise most ATIPP Coordinators if they were told they were responsible for privacy protection on the Y-drive. Before this self-audit, I doubt that any one of them considered that task to be among their responsibilities.

**[39]** There is a distinction to be drawn between (a) responsibility for ATIPP compliance, and (b) overall responsibility within the organization for privacy. Typically, ATIPP Coordinators are not senior managers. Some are entry-level employees. Most do the job as an add-on to their main job. Most ATIPP Coordinators do not have the authority, experience, training, or knowledge necessary to have overall accountability for privacy within the public body.

**[40]** HEA is a notable exception. It has a Chief Information Officer, who is a senior manager, and a Privacy Officer who reports to the Chief Information Officer. Health's answer to my question about accountability reads as follows:

> Health currently has an Access to Information and Protection of Privacy (ATIPP) Coordinator as well as a Privacy Officer. Both positions are primarily responsible for privacy and providing advice and support to Health staff and Senior Management. In addition, the Privacy Officer supports Health in developing and implementing standards, processes, and systems to ensure and safeguard the privacy and integrity of personal information held by Health.

Health added that the Director of eHealth and the ATIPP Coordinator regularly audit files on the Iqaluit Y-drive. Until this review, the audits were restricted to the Iqaluit Y-drive, but the ATIPP Coordinator now has access to all of Health's Y-drives.

**[41]** EDU says that its Manager of Information and Education Technology is responsible for all Y-drive folders and monitors all access to the Y-drive. It adds that this manager "works closely with divisional directors, principals, and other staff to ensure access to folders aligns with requirements of each position/staff member".

*b. Privacy by design*

**[42]** Technological design of the Y-drive should support the protection of personal information. In particular, the default settings should be privacy-protective.

**[43]** The self-audits show that the most fundamental problem with the Y-drive, across the GN, is that the default settings are <u>not</u> privacy-protective. The Y-drive defaults are designed to be user-friendly. There were few constraints on what staff could put on the Y-drive.

**[44]** There is a proper, privacy-protective way to set up folders and permissions on the Y-drive. To do so, however, requires special knowledge, extra time, and extra effort. It is not surprising that not all GN employees have the knowledge or are willing to put in the time or effort. That is human nature. Most of the time, we go with the default.

**[45]** Moreover, ongoing <u>maintenance</u> of folders and permissions requires even more knowledge, time, and effort.

**[46]** The fundamental idea behind "privacy by design" is that the technology should be designed to be privacy-protective. Among other things, the defaults should protect privacy. Based on the self-audits, I conclude that the Y-drive was not designed with privacy in mind.

*c. Contextual protection*

**[47]** The degree of privacy protection should be commensurate with the context. The more sensitive the personal information, the greater the protection it needs.

**[48]** Based on the self-audits, I conclude that the Y-drive is unable to distinguish between different kinds of personal information. A file is a file, and a document is a document. Any protective measures, such as password protection or access permissions, have to be added in by human intervention.

*d. Logical organization*

**[49]** The Y-drive should be organized in a standard, logical, user-friendly way. The Y-drive should use a standard numbering/naming system such as ORCS/ARCS (operational records classification system and administrative records classification system).

**[50]** The self-audits show that no public body consistently uses an organizing system for its entire Y-drive. A few (e.g. HEA) have relatively small portions of their Y-drives that use ORCS/ARCS.

**[51]** One public body described the organization of its Y-drive this way:

> In its current state, [the public body's] Y-drives are largely organized by branch, division, or section. However, there are many files and folders created that do not fit within this structure. Nested within the named program folders, information is organized in a variety of ways: topic, subject, position, employee name, by ARCS/ORCS code, by fiscal year, etc. There are a variety of organizational styles and naming conventions utilized. It is clear employees are trying to organize their records; however, there is a lack of consistency resulting in disorganization.

The self-audits show that this description could, with minor variations, be used to describe Y-drives across the GN.

**[52]** The lack of logical organization increases the risk of privacy breaches. Multiple copies of the same personal information may be placed on the Y-drive, in different folders with different access permissions, simply because a user does not realize the information is already there. Personal information may be left on the Y-drive long after it has served its operational purpose.

**[53]** I note also that, when there is no standard filing system, the Y-drive becomes English-centric. The standard systems such as ORCS/ARCS are numbers-based rather than language-based. When filing is done in the English language only, a user must be familiar with English grammar, syntax, acronyms, and abbreviations, not to mention departmental jargon.

**[54]** In a territory with three official languages, the English-centricity of the Y-drive offers another good reason to move to a standard, numbers-based filing system.

*e. Need to know*

**[55]** Files on the Y-drive containing personal information should be accessible only by those employees who need to see them to do their jobs.

**[56]** There are two dimensions to this issue. One is whether a given employee can look into the files of other operating units within the department. In my correspondence with the public bodies, I referred to this dimension as "horizontal access". The other is whether is a given employee can look into the files of a hierarchical superior, e.g. the files of management, up to and including the deputy minister. I referred to this dimension as "vertical access".

**[57]** On the Y-drive, each folder has "permissions" that dictate who can look inside the folders. The self-audits show that the permissions are often haphazard. The permissions can quickly become confused, for example, if a sub-folder is moved to a different folder with different permissions. Confused permissions – or permissions extended to an entire department – leads to problems with horizontal access and vertical access.

**[58]** The case of *Review Report 17-117 (Re)*, 2017 NUIPC 4 (CanLII) shows what can happen when user groups contain ineligible employees. A Justice employee was mistakenly added to a user group at Health, because their names were similar. The Justice employee then used this mistaken access to read and, in at least one case, share personal health information. The error came to light only when a member of the public complained.

**[59]** Moreover, the permissions are often outdated. When an employee changes jobs, or leaves the GN, there is no system for ensuring that their "permissions" are updated. This is a problem within the GN, which has many vacant positions, temporary assignments, and transfer agreements.

**[60]** The self-audits showed that many folders could be accessed by someone who is no longer in a job that requires access. Some public bodies argue that the risk is minimal, because access would require the person to have access to the same public body's Y-drive in the same community. As Review Report 17-117 shows, the risk is not always minimal or theoretical.

**[61]** As a result of the self-audits, many public bodies became aware for the first time that their Y-drive permissions needed updating. My understanding is that some of this updating has now been done. That is, in itself, a beneficial result of the self-audits.

*f. Least disclosure*

**[62]** When an employee needs to see personal information on the Y-drive, they should be able to see only the amount necessary for them to do their jobs.

**[63]** For example, in the electronic medical records system used in Nunavut, known as Meditech, scheduling clerks have enough access to Meditech to do their jobs, but they do not have access to personal medical records. That is a simple and effective way to ensure that scheduling clerks cannot become data intruders, or at least not with respect to clinical records.

**[64]** On the Y-drive, the folder permissions are all-or-nothing – either the user has full permission, or they have no permission. The Y-drive is not designed for different levels of access.

*g. Full life-cycle protection*

**[65]** Access to personal information on the Y-drive should be managed through its full life-cycle, from the time the personal information is placed on the Y-drive until its planned destruction or archiving.

**[66]** One often-overlooked protection against the risk of privacy breaches is the disposal of records, whether by destruction or archiving. The risk of a privacy breach is increased if records are held longer than necessary: see, for example, *Department of Finance (Re)*, 2022 NUIPC 10 (CanLII).

**[67]** The disposal process is governed by the *Archives Act* and the Records Retention and Disposal Authorities (RDAs) adopted under that Act. Almost all GN units have an applicable RDA.

**[68]** The haphazard organization of most Y-drives means that records are not being disposed of (i.e. destroyed or archived) in accordance with the applicable RDA. When records stay on the Y-drive beyond their useful life, there is an increased risk of a privacy breach. As I wrote in the *Finance* case (at paragraph 37) "When personal information is properly disposed of, it is no longer available to be lost or stolen".

*h. Documentation*

**[69]** There should be written policies and procedures for the Y-drive. They should be readily available to staff using the Y-drive.

**[70]** The self-audits show that most public bodies do not have a policy or procedure on how to use the Y-drive. There is, for example, no policy on what belongs on the Y-drive and what does not.

**[71]** HR holds a substantial amount of personal information about GN employees and job applicants. It has two directives (HRM 1103 Personnel Records and HRM 1104 Release of Information) to guide HR staff about the handling of personal information. Although these directives are not specifically about use of the Y-drive, they are a signal that HR is alert to the sensitivity of the personal information it holds.

**[72]** CGS, which has overall responsibility for the Y-drive, has been developing a policy suite to address information and records management. The policy suite currently consists of a Records and Information Management Policy and six associated standards. This RIM Policy is in the final review and approval process. When adopted, the RIM Policy will provide the necessary framework at the enterprise level.

**[73]** CGS may also publish an Approved Storage Location Standard prior to final approval of the RIM Policy. This standard will provide a framework to organize and control security groups, folder structure and technical configuration of the Y-drive.

*i. Audit trail*

**[74]** When there is a question about who viewed personal information on the Y-drive, an audit trail should be available.

**[75]** It is possible, at least theoretically, to determine who looked at a given file. In *Department of Community and Government Services (Re)*, 2022 NUIPC 2 (CanLII) at paragraphs 37 and 38, I wrote about the results of an audit done by JUS in the wake of my V-drive review. The audit revealed that a file containing sensitive personal information had been viewed by "a surprisingly large number" of GN employees. Without the audit, JUS would not have known that.

**[76]** But the audit procedure appears to be time-consuming and cumbersome. That may explain why almost none of the GN's public bodies completed their V-drive reviews.

**[77]** This may be contrasted, for example, with the Meditech system: see *Department of Health (Re)*, 2023 NUIPC 6 (CanLII). Meditech is another data warehouse, though better designed and better organized than the Y-drive. There is an audit trail for every action taken by a user. The audit trail can be examined, quickly and easily, should a question ever arise about unauthorized access.

*Concluding comments*

**[78]** Based on the self-audits, I conclude that the Y-drive is fundamentally flawed from a privacy perspective. The privacy problems are too pervasive to be fixed.

**[79]** At the same time, the self-audits confirm that the Y-drive is widely used throughout the GN. Every working day, many users need the Y-drive to do their jobs. From the users' perspective, the Y-drive is a success.

**[80]** This series of self-audits has raised awareness of privacy issues on the Y-drive. It has already led to some positive changes in organization and security.

Nevertheless, the people involved in the self-audits will move on, memories will fade, and new users will come along who know nothing about the self-audits. Since the Y-drive's design is not being changed, the privacy issues will persist.

**[81]** I note that CGS, when facing similar issues with the V-drive, decommissioned the entire V-drive and replaced it with a different storage system.

**[82]** I note also that FIN is currently engaged in a major project to implement an Enterprise Resource Management (ERM) system for the GN. Its primary holdings will be financial and human-resources information. I have been informally consulted by FIN as the project unfolds. I am aware that those leading the project are aware of the importance of privacy by design.

### Adoption and foster records

**[83]** Although I have, in this special report, avoided dwelling on specific public bodies and specific files, there is one situation that I believe deserves mention.

**[84]** Adoption records are, or should be, the most tightly-controlled records in Nunavut. The *Adoption Act* and its regulations lay down information-protection rules that are substantially tighter than any other statutory rules of which I am aware.

**[85]** In the course of this review, I learned that adoption and foster records held by DFS could be seen by <u>all</u> DFS employees in Iqaluit. Direct access on the Y-drive was appropriately limited. However, back-door access was available for anyone who cared to look. Why? Because <u>copies</u> of the adoption and foster records had, for different reasons, been placed in unsecured files on the Y-drive. This situation is a perfect example of how a disorganized Y-drive creates the risk of a privacy breach.

**[86]** I immediately brought my findings to the attention of DFS, in the expectation that they would move very quickly to tighten the controls over adoption and foster records.

**[87]** For purposes of this special report, I asked the DFS deputy minister for assurance that the adoption and foster records have, in fact, appropriately restricted access. The deputy minister's response, in a letter dated March 13, 2023, is as follows:

> Thank you for your letter of March 13, 2023, inquiring about whether the adoption and foster family information on the DFS Iqaluit Y-drive has been secured. I am happy to say that yes, access to the Directorate root folder, which contains the adoption and foster family information, has been restricted to employees with routine operational access to directorate files.
>
> In the second stage of our Y-drive clean-up, we are asking Directors to review the group membership lists for each subfolder within their division's root folder. With this step we will further ensure that subfolders are restricted. As mentioned in my previous letter, the second stage of the Y-drive clean-up will also include additional measures to organize, delete, move and update files on the Y-drive.

**[88]** Based on this letter and also on DFS's self-audit, I am satisfied that DFS has taken to heart the need to re-organize its Y-drive and tighten controls over the sensitive personal information it holds. I note there has been a change of deputy minister at DFS since that letter was written.

## Conclusion

**[89]** The Y-drive does not meet the "reasonable security arrangements" standard in section 42 of the ATIPPA.

**[90]** There are certain steps that a public body can take to mitigate the risk of a privacy breach on the Y-drive, but these steps, alone or together, do not meet the "reasonable security arrangements" standard in section 42 of the ATIPPA.

## Recommendations

**[91]** I understand that replacing the Y-drive is a major undertaking, with significant implications for budget and operations. **I recommend** that CGS begin or continue the planning process for the Y-drive's eventual decommissioning.

**[92]** Until the Y-drive is decommissioned, I make the following recommendations for each public body using the Y-drive:

a. **I recommend** that each public body designate a specific position as being accountable for privacy protection on the public body's Y-drives. (To be clear, I am not recommending a new position; rather, I am recommending the designation of an existing senior manager.) In most cases, **I recommend** that this designated position <u>not</u> be the public body's ATIPP Coordinator.

b. **I recommend** that each public body immediately follow through on the findings of its self-audit to restrict access to any files on its Y-drive identified as <u>high risk</u> for a privacy breach. (Some public bodies have already satisfied this recommendation.)

c. **I recommend** that each public body document its policies and procedures for its Y-drive.

d. **I recommend** that each public body consider how to follow up on non-urgent issues identified in the self-audit, taking into account the indicia of "reasonable security arrangements" discussed in this report. I recognize that how and when the follow-up to non-urgent issues occurs is an operational decision best left to each public body, to be balanced against other issues and priorities.

**[93]** **I recommend** that the Department of Executive and Intergovernmental Affairs respond to this special report on behalf of the thirteen public bodies currently using the Y-drive.

Graham Steele
ᑲᒥᓯᓇ / Commissioner / Kamisina / Commissaire