



To: Graham Steele

Office of the Information and Privacy Commissioner of Nunavut
PO Box 1000, Station #270
607 Queen Elizabeth II Way
Iqaluit, Nunavut, X0A 0H0
admin@atipp-nu.ca

March 1, 2022

Response To Information Privacy Commissioner Review Report 22-211-RR

Dear Mr. Steele,

Thank you for your Review Report 22-211-RR on the Government of Nunavut (GN) V: drive privacy breach.

This letter is to provide a response to your review and provide you with the key steps Community and Government Services (CGS) will be taking going forward in response to this incident.

A Pre-Privacy Impact Assessment (PPIA) has been initiated to specifically address this new file sharing solution to ensure that any privacy vulnerabilities that may be associated with it are identified and mitigated. (Further details will be provided on this new file sharing solution in the PPIA).

While we have communicated the primary solution to the V: drive problem, which was to replace the V: drive entirely (the V: drive itself has already been decommissioned GN wide), the real solution itself will be utilizing an enterprise-wide file sharing solution. This was implemented in January 2020 and is now being utilized by all GN departments. This new enterprise-wide file sharing solution follows many best practices for data security; however, we have incorporated several other factors which add additional layers of protection to our data.

The first is two-factor authentication. This will stop anyone from accessing GN files even if they obtain an account password. For example, if a thief accesses a computer with a saved password, your phone acts as a second form of authentication by calling the account holder for a secondary confirmation of the account login.



Secondly, the GN has rolled out Yubikey which is a USB device that plugs into your computer and, along with your password, completes the second half of a Multi Factor Authentication (MFA) account login. It protects from phishing and advanced man-in-the-middle attacks, where someone tries to intercept a user's two-factor authentication.

Your two recommendations are currently being acted upon:

- 1) As you accurately stated in S. 46 of your review, "CGS is not responsible for ensuring that public bodies comply with their statutory obligations under the ATIPPA". As such, CGS will be working with the Territorial ATIPP Manager to provide him with any assistance he requires to support his efforts to bring all of the GN public bodies into compliance with the ATIPP Act and completing and processing any breach report submissions from the various GN departments needed to fulfill the GN's obligations regarding the processing and reporting on all V: drive files outstanding in this matter. Of course, CGS will also complete its own work on any outstanding V: drive files and where appropriate, privacy breach reports will be completed and forwarded to your office.
- 2) CGS is currently using the tracking system developed by the Territorial ATIPP Manager.

We will be working closely with the Territorial ATIPP Manager to ensure that CGS is in full compliance with our statutory obligations under the ATIPP Act.

Please feel free to reach out to me if you have any questions or concerns regarding this matter.

Sincerely,

P.J. Akeegok
Premier of Nunavut

Hon. David Joanasi
Minister, Community and Government Services

cc:

Jimi Onalik, Deputy Minister, EIA
Kyle Seeley, Deputy Minister, CGS
Yuri Podmoroff, Territorial ATIPP Manager, EIA
Chris McNeil, Security and Privacy Policy Analyst, CGS