Information Security
UNIVERSITY OF TORONTO

Office of the Chief Information Security Officer

Interpretive guidance on handling of social insurance numbers (SINs)

Effective: Dec. 13, 2023

Purpose

The purpose of this interpretive guidance is to clarify the University of Toronto's Information Security Control Standard as it applies to the collection, storage, processing and sharing of social insurance numbers (SINs) by the University.

Preamble

Based on the Data Classification Standard, SINs are level 4 data, and in combination with other personal information could lead to identity theft. Collection, storage, processing and sharing of SINs must be done in a secure manner and in accordance with U of T's Information Security Control Standard and Freedom of Information and Protection of Privacy Act (FIPPA) requirements. The existence of level 4 data, like SINs, on email platforms creates an unacceptable risk in the event of a compromised, misdirected or improperly forwarded email.

Scope

This interpretive guidance is authorized under the Policy on Information Security and the Protection of Digital Assets and inherits the scope. The policy applies to all academic and administrative units, third-party agents of the University, as well as any other University affiliate that is authorized to access institutional data, services and systems.

SIN collection, storage and sharing requirements

1. SINs must only be collected and used for financial and taxation purposes and as required by the government of Canada.
2. SINs must not be used as a method of identification unless legally authorized.
3. Before collecting SINs, a notice of collection must be provided.
4. SINs must not be collected over email in unencrypted form.
5. SINs must not be shared or stored within the University email system in an unencrypted form.
6. SINs must be stored only in authorized systems (no shadow copies).

Secure methods of SIN collection:

1. Collect directly into a secure system capable of handling level 4 data.
2. Collect verbally and enter directly into a secure system capable of handling level 4 data.

Systems used to store or process SINs must meet the requirements for level 4 data set forth in the Information Security Control Standard, including but not limited to the following:

1. Data must be encrypted at rest.
2. Data must be encrypted while in transit.
3. System must have gone through a security risk assessment and any identified risks must have been appropriately addressed.
4. Access to the system must be restricted to a need-to-know basis.
5. Access must use multi-factor authentication (MFA).

Related resources

- Information Security Control Standard – U of T Information Security
- Data classification – U of T Information Security
- Policy on Information Security and the Protection of Digital Assets – Office of the Governing Council
- SIN code of practice – Government of Canada

Endorsed by the Information Security Council on Dec. 13, 2023.