

Safeguarding Personal Information

Personal information must be protected by making reasonable security arrangements against unauthorized access, use, disclosure, or destruction.

3 Types of Safeguards

Physical

Actual physical controls in place to prevent or limit access to any location where personal information is used and/or stored

Examples: Locked cabinets, secure building entry, video security, biometrics, etc.



Technical

Automated security measures & processes to protect personal information at rest and in transit, from unauthorized access, use or disclosure

Examples: Data encryption, firewalls, multi-factor authentication, network security, disaster recovery, vulnerability assessments, etc.



Administrative

Organizational measures to manage the protection of personal information and the conduct of employees and vendors in relation to protecting that information

Examples: Policies and procedures, training, data sharing agreements, privacy officer, breach protocol, etc.



Safeguard Reasonability Test

When evaluating the 'reasonableness' of privacy and information security safeguards, consider the following questions.

Are the safeguards...

- proportionate to the sensitivity of the information?
- adequate, given the potential harm should a breach occur?
- applicable to the entire lifecycle of the information?
- protecting privacy without being cost prohibitive?
- enabling a quick and efficient response in the event of a breach?
- documented in policies, procedures and standards?
- clearly communicated to vendors as requirements in contracts?

Thanks to the Nova Scotia Office of the Privacy Commissioner – 'Reasonable Security Checklist for Personal Information'