Privacy and Security Framework Overview

The Canadian Partnership Against Cancer (The Partnership) has a broad reaching mandate to implement Canada's cancer control strategy by bringing together the efforts of partners across the country and by working with cancer experts, charitable and national health organizations, governments, cancer agencies, survivors and others. In executing its mandate, the Partnership collects, stores and shares vast amounts of information with various sensitivities and has developed an equally robust information security program.

The Partnership's Privacy and Security Framework

The Privacy and Security Framework (Figure 1) forms the basis of the Partnership's robust information security program, encompassing a broad array of information technology standards and policies. All of the Partnership's information technology and Information management standards and policies are modelled after industry standards and are designed to inform and guide a broad range of IT security related activities across the portfolio of work at the Partnership. The information security program positively impacts the entire organization, with systems security activities and operational guidance that support daily and strategic business operations, as well as consultation, technical, and policy oversight to various project activities that leverage the Partnership's corporate information systems.

The information security program is managed and delivered under the authority and stewardship of the Chief Privacy and Security Officer and the collective Corporate Services Department within the Partnership. Reporting on monitoring and compliance to the Privacy and Security Framework is presented annually to the Partnership's Finance and Audit Board Committee.

10 core elements of The Privacy and Security Framework

1. *A comprehensive and expanding group of systems' security policies*, which provide guidance on a wide array of security-related matters
2. *Annual review of all the Partnership security related policies*, to ensure ongoing relevance and efficacy
3. *A customized systems security training program*, delivered via on-line computer based training, which includes annual training sessions for all staff, as well as orientation sessions for new staff
4. *Threat Risk Assessments (TRA)*, carried out on all new and significantly revised Partnership information systems, and remediation activities arising from these assessments managed through safeguard implementation plans
5. *An active risk management program* that tracks and monitors the implementation of security controls and risks within the organization's corporate information systems
6. *Comprehensive periodical reviews of user access* to the Partnership's most sensitive corporate data holdings
7. *IT Change Advisory Board* that consists of key members of the Partnership's IT Department, external vendor IT expertise and expertise from external IT security personnel and program managers as required, to ensure that the requested changes to the systems are thoroughly checked and assessed from both a technical and business perspective to minimize risks

8. *Security reviews* in the Partnership's systems review process, to ensure early detection of potential security-related issues, determine the level of risk associated with those issues, and make informed decisions about risk mitigation or acceptance

9. *Ongoing maintenance and enhancement to the Partnership's corporate information systems* including enhanced network security, segmentation and access control, to minimize and mitigate any potential security risks

10. *Introduction of new centralized identity management and access control technologies*, to offer a high degree of assurance on user level access throughout the organization and public facing services

The Information Technology Support at the Partnership

The Director of Information Technology is responsible for the management of information security at the Partnership and in guiding the information security strategy. Reporting to the Chief Privacy and Security Officer, the Director of Information Technology advises on information security policies around strategic initiatives, technology architecture and systems security matters.

The Department of Information Technology under the guidance of the Director of Information Technology is staffed with two full time IT managers and a team of architects, analysts and web developers who are dedicated to the efficient and cost-effective management of the Partnership's corporate information systems.

The Partnership also relies on a dedicated team of external industry security experts, available on demand, for conducting discrete and more complex security assessments, providing guidance on policy, systems architecture, operational practice and information security as a whole. Leveraging vendor's expertise, in concert with internal and external resources, the Partnership has focused on over-arching security matters, related to corporate infrastructure, audit, and risk assessment on new and existing projects.