Contact us

Email: OCIOSecurity@gov.bc.ca

Visit our website: **http://www.gov.bc.ca/informationsecurity**

Security Tips

Protect the information in your possession, at work, on the go and at home. With more flexible work arrangements and the use of mobile devices, following are some basic information security tips to remember.

- Never share your credentials (IDIR ID and password, or any other account names and passwords) with anyone.
- Consider storing information on shared drives or in SharePoint Workspaces where it can be accessed by others.
- Use the Delegate option in iProcurement or iExpenses to allow someone to act on your behalf.
- Use Permissions and/or the Delegate option in Outlook to allow others access to your mailbox.
- Create strong passwords and try to not use the same access password twice. Never use your IDIR password outside of work.
- Consider using passphrases: “to be or not to be” becomes tBoN2b.
- Do not click on any links or attachments in emails that are not from a trusted source.

Each ministry has a Ministry Information Security Officer (MISO) who is the single point of contact for information security issues.

The **Security News Digest**, produced weekly by the Information Security Branch, is a compilation of stories about current security breaches, threats and risks, results of research by top security specialists, and social trends on the use and abuse of technology, emailed to subscribers weekly. Contact OCIOSecurity@gov.bc.ca to subscribe.

Information Security Branch

Enabling Secure Business

BRITISH COLUMBIA

OCIO | Office of the Chief Information Officer

Threats to Information?

An actual or suspected security or privacy breach, which includes the collection, use, disclosure, access, disposal, or storage of personal or sensitive business information, whether accidental or deliberate, that is not authorized, needs to be reported.

Follow the Information Incident Management Process – immediately report it to your supervisor or management contact, who must then call the Shared Services BC Service Desk at 250 387-7000, or toll-free at 1-866 660-0811 (available 24/7) and select option 3 – state that an Information Incident Investigation is required. The appropriate response will follow on from there. When in doubt, it is better to report your suspicions.

Security is Everyone's Responsibility

The **Office of the Chief Information Officer** is responsible for the security of government's information and for developing the policies, standards and programs that protect sensitive and personal information.

The **Information Security Branch** provides the overall governance for information security supporting the secure delivery of government programs. The branch is comprised of various components of security that work together to bring value-added service to its clients.

Information Security Program

Promotes a risk-based approach to information security that supports government in achieving its goals.

Ensures programs, plans and processes are in place to appropriately manage information security risks to an acceptable level.

About us

The **Security Awareness** team creates an awareness of information security threats, risks and best practices for government and the Broader Public Sector by way of events and published materials in support of the protection of information.

Advisory Services provides subject matter expertise by way of consulting services across government on new technology and major initiatives. The Unit also manages Government's Information Security Program and Information Security Policy, conducts security audits or reviews as required and also develops and provides advice on information security standards and architecture.

The **Investigations and Forensics** Unit leads the investigation of all reported breaches (actual and potential) of information security, including information incidents and cyber security events. The Unit also provides investigative and forensic services to other parts of government, supporting a broader range of policy and legal issues.

The **Security Operations** Unit architects, designs, implements and supports a number of operational security services, including Firewall/Access Control, Content Filtering, Intrusion Protection, Application Scanning, Denial of Service protection, and a Security Information and Event Management (SIEM) service. Additionally, the Unit provides physical security support and IT security consulting to other groups.

The **Access and Directory Management Services** team provides the directory infrastructure and ID administration services for all Government staff and many Broader Public Service (BPS) organizations. The team also operates Government's web access management and single sign-on environment, enabling Government programs and BPS organizations to securely deliver their online services to citizens, businesses, and staff.

The **Vulnerability & Risk Management** team provides the framework and support for information security compliance management, including providing tools and training to ministry information security staff to support the risk management process. The Unit manages government-wide information security assessment activities using iSMART and key information security risks through tracking and reporting on all known security issues which pose a risk to government information