Applications and Software

Privacy and Security Considerations

Applications are a part of our everyday lives; they are used for everything from getting weather reports and directions to tracking our fitness levels and health. Increasingly, applications are becoming part of our professional world as well, helping to increase productivity and facilitate collaboration. At the same time, the Workstation Refresh Project has increased the flexibility that employees have in managing their devices. Employees now have greater choice in the tools that they can use to do their jobs, including which applications and software are used.

While applications and software provide us with additional tools to do our jobs, employees need to be aware of the potential risks to privacy and to the security of government information when using applications and software. Not every application is safe to use for work purposes. As well, some applications and software may impose terms and conditions that are unacceptable to government.

For these reasons, the Appropriate Use Policy requires that employees obtain their supervisor's permission before downloading applications or software to their device. This includes downloading applications and software to a workstation as well as to a mobile device, such as a laptop, smartphone or tablet. The requirement to obtain supervisor permission is not meant to be a deterrent to downloading useful applications and software. Rather, it is to ensure that applications and software are downloaded with full knowledge of both their benefits and potential risks.

Ministries may develop specific policies or guidelines to assist supervisors in determining the safety and suitability of applications and software. In the meantime the following guidelines will assist supervisors with this assessment.

Application and Software Checklist

If you answer "Yes" to any of the following questions, there may be privacy or security concerns and it is recommended that you seek further advice or direction.

	Ask yourself	Yes	No
Privacy	If you answer "Yes" to any of the following privacy related questions it is recommended that you contact the OCIO's Legislation, Privacy and Policy Branch at **Privacy.helpline@gov.bc.ca** or 250-356-1851		
1.	Will you be using the application or software to store or send any personal information? • For example, are you planning to use an application like DropBox to send files with data about individuals, or will you be using Siri to translate client testimony?		
2.	Will the application or software have access to anyone else's personal information, such as their names, personal addresses, and personal phone numbers? • For example, many applications will want access to your Contacts or Address Book. **Note: If the application has an opt-out or decline option on this access, and you will opt out/decline, you may answer "No" to this question.**		
3.	Does the application have settings that allow it to share information with other applications? • For example, many applications will want to "connect with your Facebook friends" or link to your contacts in another application/online service. **Note: If the application has an opt-out or decline option for these connections, and you will opt out/decline, you may answer "No" to this question.**		
Security	If you answer "Yes" to any of the following security related questions it is recommended that you contact your Ministry Information Security Officer (MISO)		
4.	Will the application or software have access to any confidential government information? • Confidential information includes personal information and other information with confidentiality requirements such as Cabinet confidences, third party business information, confidential advice and recommendations, contract negotiations, and legal advice. Information classified as "sensitive" for the purposes of security classification should also be considered confidential.		
5.	Does the application require unnecessary or inappropriate access to the network? • In some cases, an application will require access to the network in order to function properly (e.g., search engines and social media). Other applications (for example games, compasses, and calculators) should not require network access to function. An application may ask for network access so that it can download required updates, but network access can also be used to transfer information off of the device. • If the application is asking for access to the network, you should ask yourself whether the application needs that access to perform its intended task. If it doesn't, the application could be putting the network at inappropriate or unnecessary risk. If you need assistance in making this determination, you should contact your MISO.		
6.	Are you aware of any concerns about the application's reputation?		

Ask yourself	Yes	No
• For example, some application stores or providers (e.g., Android) do not currently vet their applications to the same degree as others. While this does not mean that these applications are not safe or suitable (to the contrary, many of these applications are perfectly safe and useful), it may, at least for the near future, warrant some additional consideration. **Note: if you have no information on the reputation of the application or its manufacturer, the following sources may help:** • Do an internet search of the application and the manufacturer • Check out user reviews of the application • Ask your colleagues or Ministry Information Security Officer		
7. Is there anything about the application or software, not already addressed above, that concerns you? • Services available on devices and the threats to devices, privacy and information change all the time and cannot all be addressed in a guidance document such as this. For this reason, if there is anything about the application or software that concerns you or makes you uncomfortable, you should seek advice from your Ministry Information Security Officer.		

Further Considerations:

Generally speaking, it is good practice to remove old applications and software from your device when you are no longer using them. This helps the device to run more efficiently, and also helps ensure that the minimal amount of information that is needed is accessed.

For information about the Appropriate Use Policy contact:

IM IT Policy and Legislation Branch
Im.itpolicy@gov.bc.ca