



Working With Sensitive Information

Compromised information has potential to do real damage to Canada, the Department of National Defence (DND) and the Canadian Armed Forces (CAF).

Such as:

- Loss of confidence in the DND/CAF
- Put the safety of military and civilians in operations at risk
- Damage Canada's trustworthy reputation nationally and internationally



Is your information Classified or Protected? Try this test

INJURY TEST

If this information were compromised, it could cause...

No injury	Injury to the national interest	Injury to some interest, but not the national interest
UNCLASSIFIED	CLASSIFIED	PROTECTED
AGGREGATION OF INFORMATION If information is bundled together, the bundle may be more sensitive than its parts. For example, a file containing one address may be Protected A, while a file containing 10,000 addresses would be at least Protected B. This is known as the aggregation of information.	The injury caused by the compromise of the information would be...	The injury caused by the compromise of the information would be...
	An injury → Confidential	An injury → Protected A
	A serious injury → Secret	A serious injury → Protected B
	An exceptionally grave injury → Top Secret	An exceptionally grave injury → Protected C

! Need-to-Access and Need-to-Know

Access to sensitive DND/CAF information **must be limited to authorized individuals whom:** have the appropriate security clearance/reliability status, and a need-to-know. Nobody is entitled to access information because of rank or security clearance/reliability status.

i Loss of Sensitive Information

If you know or suspect that **sensitive information (including Cabinet confidences) has been lost or compromised**, contact your USS, ISSO or DGDS Security Incident Management (**++DGDS SIM-GIS@VCDS DGDS @Ottawa-Hull**), who will work to contain and mitigate the loss.

WHAT TO DO:

- ✓ **Sensitive information must be marked as soon as it is created.** Add security markings at the top and bottom of each sensitive document.
- ✓ Sensitive files must be moved in folders **appropriate to their sensitivity level.**
- ✓ **Secure sensitive documents and computer media (such as CD's, DVDs, USB keys or other media)** in approved security cabinet when not in use.
- ✓ Ensure that cabinets, safes and other security containers are **locked at the end of the day.**
- ✓ Sharing with another government department **may be governed by MOU.**
- ✓ **Did you know** that security, including storage, for portable electronic devices is addressed in the **DND/CAF Information Technology Security Standard for Portable Information Technology Devices (ITSS-01)?**

When in doubt, consult with your ISSO

Further details are available in NDSODs Chapter 6: Security of Information, and the Security of Information Standards.

WHAT NOT TO DO:

- ✗ **Do not** leave sensitive information unprotected when away from your desk.
- ✗ **Do not leave Protected B documents at the printer.** Retrieve them immediately without delay.
- ✗ **Do not remove sensitive information** from the applicable secure zone without justification and permission from the approved authority. **Refer to transport and transmittal requirements located in NDSOD Chapter 6: <https://collaboration-admpa.forces.mil.ca/sites/DI/SafetySecurity/vcds-ndsod-c06.pdf>**
- ✗ Material that **has contained sensitive information must not be disposed** of through federal or municipal recycling programs, unless it has been properly destroyed prior to recycling.
- ✗ **Do not process sensitive information on non-approved equipment such as using the DWAN to process classified data.** *E.g.: Sending SECRET information from the DWAN.*
- ✗ **Do not share or discuss sensitive information in public, with anyone who does not have a need-to-know and proper security clearance.** The fact that information is Unclassified does not mean that it is open to the public or to DND employees or CAF members without a need-to-know. Approved release procedures must be followed.

