



See It, Hear It, Suspect It – **Report it**

What is a security incident?

Any event, act or omission that could compromise DND/CAF, information, services or assets.

Let's break it down:

Security incidents fall into two categories:

1 Violation

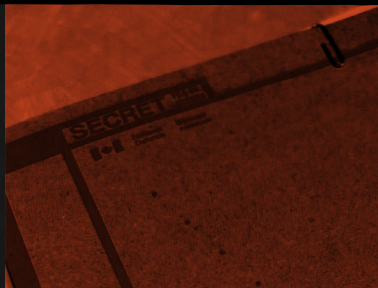
A rule is broken (*deliberately or accidentally*) but **no sensitive information (Classified, Protected or assets)** is compromised.

2 Breach

is a **violation of sensitive information** that leads to actual or potential compromise (*accessed or exposed*).

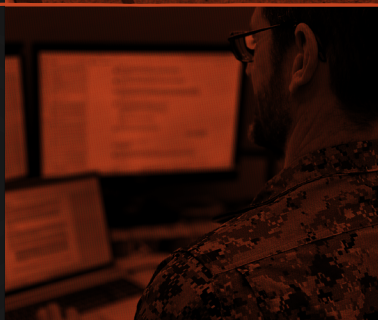
This happens more than you think:

An employee leaves a **SECRET document on their desk** in a High Security Zone (HSZ), and no one has seen it.



An employee leaves a **SECRET document on their desk** in a HSZ. A colleague without the required clearance or need-to-know walks by and reads it.

An employee uploads an **unencrypted PROTECTED B document to SharePoint**, but it's removed before anyone views or downloads it.



An employee posts a **PROTECTED B document in a large unit group chat on Teams***. It's deleted later, but several colleagues without the need to know viewed and downloaded it.

**Sharing PROTECTED B files on MS Teams is always prohibited.*

A CAF member **discusses protected deployment information** in a coffee shop while in uniform. No one overhears.



A CAF member **discusses protected deployment information** in a coffee shop while in uniform. A nearby stranger without a clearance or need-to-know overhears.

Rules were broken, but information was not compromised.

Information has been compromised.

If in doubt

take immediate mitigating actions (*within your authority*) to contain the incident and prevent further damage.

Report either to:

- ▶ Your Chain of Command
- ▶ Your Unit Security Supervisor (USS)
- ▶ Your Information System Security Officer (ISSO)
- ▶ Area, Formation, or Local Help/Service Desk
- ▶ Your local Military Police

For more information:

- + Contact the Security Event Management (SEM/SIM) Section via DWAN, CSNI, or SPARTAN
- + National Defence Security Orders and Directives NDSOD [Chapter 12: Security Incident Management](#)