National Defence / Défense nationale

VICE CHIEF OF THE DEFENCE STAFF

DIRECTOR GENERAL DEFENCE SECURITY

Security Incident Management *(SIM)*

The SIM Section is responsible to the Director Defence Security Operations (DDSO) and manages security incidents on behalf of the Chief Security Officer (CSO) for the Department of National Defence (DND) and Canadian Armed Forces (CAF). The SIM Section serves as the overall functional authority for security incident management for DND/CAF by coordinating the response to incidents among all stakeholders, while ensuring investigations are actioned as deemed appropriate.

What is a Security Incident?

Any workplace violence toward a DND employee or CAF member, any act, event or omission that could result in the compromise of DND/CAF information, assets, resources or services. Security violations and security breaches are considered security incidents.

The difference between a security violation and a security breach?

1. An act or omission, deliberate or accidental **that does not result in the actual or possible compromise** of Classified or Protected information or assets is a : **SECURITY VIOLATION**
2. An act or omission, deliberate or accidental, **that does result in the actual or possible compromise** of Classified or Protected information or assets is a : **SECURITY BREACH**

Security Pillars

- Information Technology Security
- Physical Security
- Security of Information
- Safety & Security of Employees

Types of Security Incidents

- Cyber, COMSEC, EMSEC, TRANSEC, Security & Social Media
- Access Control, Critical Incidents, Security on Deployed Operations, Defence Security & Force Protection, Sensitive Inventory & Controlled Goods (ITAR/CTAT), Security of Arms, Ammunition & Explosives
- Security of Information & Assets, Personnel Security, Personal Information & Privacy, Special Access Information, Sensitive Compartmented Information
- Industrial & Contract Security

The Security Incident Management Process:

1. **Detection** – Identify security incidents at the earliest possible opportunity.
2. **Reporting** – Inform all stakeholders *(including your chain of Command)* that a security incident has occurred.

   **Report to DGDS all security breaches involving matter categorized as Protected B or higher or rated as high or very high on the impact severity matrix IAW NDSOD Ch. 12, Annex B: Impact Severity Matrix.*

   **Report to CFNOC all IT security incidents IAW IMS 6003-1-1.*
3. **Mitigation** – Stop and contain the security incident in order to prevent further damage.
4. **Investigating & Assessing** – Establish the facts, timeline and circumstances *(who, what, where, when, how and why)*, identify all the stakeholders, determine whether the security incident is a breach or violation, identify mitigation actions, assess the severity and the impact of the damage.
5. **Remediation** – Address the cause(s) and effect(s) of the security incident in order to prevent recurrence and repair any damage caused.
6. **Learning** – Incorporate the lessons observed to improve security safeguards and improve the protection of personnel, information, assets, resources, operations and services

FOR MORE INFORMATION

Reporting a security incident:

THE SIM SECTION:
DWAN: DGDSSIM-DGSDGIS@forces.gc.ca
CSNI: VCD.DGDSSIM-GIS@forces.cmil.ca
SPARTAN: DGDS_SSIMGIS@spartan.mil.ic.ca
613-947-9212

- To your USS or ISSO, as appropriate.
- To your supervisor, manager or Chain of Command.
- To your Regional Departmental Security Officer (RDSO).
- To your local Military Police (MP) Detachment.

National Defence Security Orders and Directives (NDSOD) – Chapter 12: Security Incident Management
IMS 6003-1-1 – Information Technology Security Incident Management

A-SJ-007-000-DA-110 OPI: DGDS 2022/07

SECURITY NEVER TAKES A BREAK. | VIGILANCE!

Canada