s 22 - Out of scope

4 Identifying a Critical Security Incident

A **critical** security incident is any incident where a staff member is in immediate fear for the safety or wellbeing of themselves, another staff member, a client and/or a member of the public. Examples of critical security incidents can include;

- Instances of harm to one's self or others
- A direct threat of harm to one's self or others
- Violent, antisocial and/or aggressive behaviour
- Emergency incidents (such as bomb or chemical threats)

Critical incidents may be provided by various sources, including:

- Veterans
- Defence force members
- Family members of a veteran
- DVA staff
- General public

Critical incidents may be reported / provided by a variety of methods, such as:

- Telephone
- In person
- Letters
- Emails

Critical Incidents can occur at:

- DVA tenancies or their vicinity
- Official functions and events
- Home visits
- ADF sites

s 22 - Out of scope

3. Security Incident Definitions

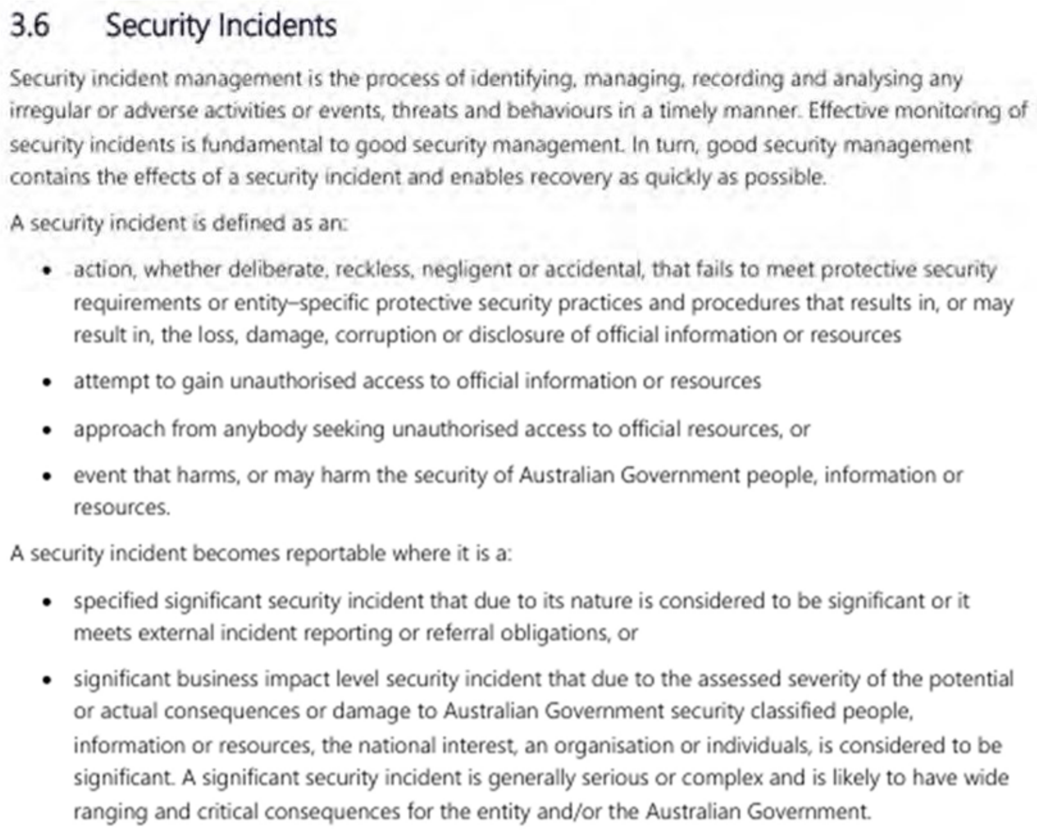
The Protective Security Policy Framework (PSPF) defines *security incident management* as the process of identifying, managing, recording and analysing any irregular or adverse activities or events, threats and behaviours in a timely manner[1].

3.1 Security Incidents

DVA defines a *security incident* as an event or circumstance that potentially, or actually, has adverse consequences for the safety and security of staff and contactors, veterans and members of public, as well as departmental information or assets. Security incidents can include the following events;

- Client or member of the public who has made direct threats to harm to DVA staff, veterans, members of the public or assets.
- Release/loss of sensitive information (including client information) to unauthorised individuals. For example, the compromise of client data or loss of sensitive documentation on a department program that is yet to be announced to the public.
- Loss, compromise, suspected compromise, theft or attempted theft of classified equipment.
- Criminal actions such as actual or attempted theft, break and enter, vandalism or assault.
- Sensitive and security classified material not properly secured, stored or disposed.
- Unauthorised use of a building access pass.
- Compromise of keys to security locks, or of combination settings.
- Sharing of ICT access passwords.

[1] https://www.protectivesecurity.gov.au/system/files/2021-08/PSPF-policy-2-Management-structures-and-responsibilities.pdf



3.6 Security Incidents

Security incident management is the process of identifying, managing, recording and analysing any irregular or adverse activities or events, threats and behaviours in a timely manner. Effective monitoring of security incidents is fundamental to good security management. In turn, good security management contains the effects of a security incident and enables recovery as quickly as possible.

A security incident is defined as an:

- action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or entity–specific protective security practices and procedures that results in, or may result in, the loss, damage, corruption or disclosure of official information or resources
- attempt to gain unauthorised access to official information or resources
- approach from anybody seeking unauthorised access to official resources, or
- event that harms, or may harm the security of Australian Government people, information or resources.

A security incident becomes reportable where it is a:

- specified significant security incident that due to its nature is considered to be significant or it meets external incident reporting or referral obligations, or
- significant business impact level security incident that due to the assessed severity of the potential or actual consequences or damage to Australian Government security classified people, information or resources, the national interest, an organisation or individuals, is considered to be significant. A significant security incident is generally serious or complex and is likely to have wide ranging and critical consequences for the entity and/or the Australian Government.

Pg. 12 Australian Government Protective Security Policy Framework

Release 2025