ADF CADETS
SECURITY FOR SUPERVISORS

Supervisors and security

Everyone in the Australian Defence Force (ADF) Cadets needs to be security conscious, and supervisors need to set an example for their cadets and adult members. As a supervisor of volunteers, your ultimate goal is to cultivate an environment in which effective security practices are embedded into your cadet unit's culture.

Promoting and practising proper security

Supervising includes monitoring security issues and practices. Security aims to protect people and assets. It should be part of everything you do.

You are the best source of information about your cadet unit's activities and knowledge of security. As a supervisor you are responsible for ensuring all ADF Cadets members know how to fulfil their security obligations.

Your key responsibilities include:

1. **Be aware of the different security risks in your unit:**

2. **Understand and communicate the importance of security procedures and practices to cadets and adult members of your cadet unit**

3. **Help your members understand their security responsibilities**
   - Educate your members on security protocols, e.g. what to do in a lockdown, how to report a security incident, how to use CadetNet appropriately
   - Deal with poor security practices and behaviours within your cadet unit promptly
   - Provide all your cadets and adult members with access to the *ADF Cadets Guide to Security for volunteers*
   - Identify unauthorised visitors and enable your members to do the same
   - Adhere to the requirements of the respective SAFEBASE level, and
   - Understand what each level means for your unit

4. **Be supportive of security**

As a supervisor, you play an important role in embedding a strong security culture. Cadets and adult members will take their lead from you, so you should:

   - Maintain a positive attitude to security and be seen to practice good security regularly
   - Make sure your cadets and adult members are aware of their individual security responsibilities
   - Acknowledge your cadets and adult members when they demonstrate good security practice

5. **Apply the need-to-know principle**

Cadets and adult members do not have access to classified Defence information. However, you should confirm that cadets and adult members are aware that their information, such as emergency procedures and base layouts, CAN be sensitive. If people ask cadets and/or adult members to share this information, they should consider if the person really needs to know it. No information should be shared without prior approval of the respective ADF Cadets Headquarters.

6. **Make sure your cadet and adult members are aware of their security reporting responsibilities**

Ensure that cadets and adult members are aware of their responsibility to report security incidents to you. You have the responsibility to follow the reporting policy and procedures for your cadet organisation and inform your manager or commander.

Protective security measures - people

Protective security measures for people ensure that only authorised people have access to Defence's information, particularly sensitive and classified information and resources. For ADF and Australian Public Service (APS) employees of Defence this is done by the security clearance process. This regular check ensures only suitably cleared people can access Defence's classified information.

ADF Cadets members are NOT required to undergo a security clearance process because they do not handle classified information. ADF Cadets are however an integrated

component of many Defence sites, and therefore have a responsibility for protective security measures related to the sharing of information with other people and who they bring on to Defence bases. This is especially true in identifying trusted insider threats.

The trusted insider threat

A trusted insider is someone who has inside knowledge of Defence and how it operates and uses this to undertake hateful and/or disruptive acts. These acts may be premeditated or inadvertently caused through poor security practices, such as not reporting a lost cadet pass. Defence's best weapon against trusted insiders is vigilance.

Examples of an insider threat may include:

- a civilian friend of an ADF Cadet asking the cadet about the weapons, firearms and/or ammunition stored in their cadet unit and/or
- an acquaintance asking an ADF Cadet member how they get onto a Defence base and where their unit is located within the Defence base

There are five main types of Trusted Insider activities:

- unauthorised or accidental release of sensitive information
- corruption of processes
- helping someone access Defence's assets without the appropriate authorisation
- physical sabotage
- digital or cyber sabotage

The best way to prevent these acts from occurring is to ensure that everyone is aware of their security responsibilities and reporting concerning behaviours, such as:

- increased nervousness or anxiety
- Saying bitter and/or angry things about Defence
- Repeated request for access to cadet weapons, firearms , ammunition and/or attractive sellable items such as laptops
- unusual interest in sensitive or classified information
- saying something or doing something that just doesn't seem 'right'

If your cadets or adult members observe any of these types of behaviours, they should report it to you. You should then report it on to your manager or commander and follow the reporting policy and procedures for your cadet organisation.

Identifying people at risk

In order to support your cadets and adult members to pre-emptively detect security risks, it is important you get to know the members of your unit so they feel comfortable discussing security concerns with you.

A person at risk may be:

- a former disgruntled ADF Cadets adult member
- an ADF Cadets member with financial issues
- an ADF Cadets member who accidentally or unknowingly discloses sensitive information

Protective security measures - Information

ICT security

Information and Communications Technology (ICT) improves movement, convenience and productivity in our daily lives. However, these benefits must be balanced against the fact that any device or computer network connected to the Internet is also vulnerable to malicious cyber activity, such as covertly collecting our information.

As cyber intrusions become more sophisticated, so too do security techniques. There is no easy solution for information security, and security products alone are not an effective solution. It is also important to remember that not all cyber or ICT threats are external. Be aware that ICT systems are also vulnerable to the trusted insider threat.

Appropriate Education on the safe use of ICT is the key to Information Security

As a supervisor, you are responsible for ensuring your cadets and adult members are educated in security and understand the potential cyber security threats to Defence. It is important that you lead by example, promoting positive ICT security practices and behaviours within your unit.

Socially engineered emails and messages

SPAM, the electronic equivalent of 'junk mail', includes electronic mail as well as mobile phone messaging such as SMS and MMS. Phishing emails are fraudulent email messages used to trick you into disclosing personal information or into releasing malicious software onto your computer or personal device. Spear-phishing emails target specific individuals or groups. While these socially-engineered emails can be highly sophisticated, there are ways to differentiate them from legitimate emails. When reading emails, be vigilant about what is entering your inbox.

- • Do you really know who is sending you the email?
- • Are you expecting an email from them?
- • Is the content of the email relevant to your work?
- • Does the email ask you to access a website or open an attachment?
- • Is the web address relevant to the content of the email?
- • Is the email from a personal email address?
- • Is the email suspiciously written?

If you have received unwanted SPAM, do not open any attachments, click on links or reply. Simply delete and empty your 'deleted items' box.

Unauthorised connections to Defence ICT systems

Do not connect any unauthorised device to a Defence system. The improper use of USB drives, smart phones and other unauthorised connections can put Defence information and systems at risk. Many devices are targeted by virus writers as a means of spreading malicious programs. Even brand new drives can be infected during manufacture. Before connecting any device to a Defence ICT system, you should speak with your manager or commander to ensure that you have an appropriate authorisation.

Staying safe on social media

With four out of five Australians online using social media it has become a popular way for enemies to gather information on Defence activities, information and people. As a supervisor, you need to ensure that your cadets and adult members understand the implications of their social media interactions.

Talk to your cadets and adult members about being social but secure online. Points to discuss include:

- Members should not post pictures of Defence sites, members, supervisors, or managers without prior permission
- Check the privacy settings for public websites; often they will collect and use your personal information
- Be aware that people may disguise their real identity online
- Members should also be aware that what they post online reflects not only on themselves, but also on their cadet unit, cadet organisation, their parent Service and Defence
- To avoid posting personal information where possible

Go to www.defenceyouth.gov.au for more information on cyber security and securely using social media.

X marks the spot: geo-tagging

Geo-tagging is the digital association of photographs with a geographical location.

Many smartphones and some digital cameras use Global Positioning System (GPS) location services which tag images with the latitude and longitude where a photo was taken. As a result, people often unwittingly share too much information about their location when taking photos or videos with their smartphone and personal devices, posting them online or sharing images via Short Message Service (SMS).

People can use geo-tagging information to pinpoint the location of people, assets and units. It can establish a person's daily routine, and can allow for undetected social surveillance.

Encourage your cadets and adult members to avoid the risks of geo-tagging by disabling this feature on their smartphones and personal devices.

To turn GPS data off, refer to the phone's settings menu and then either the "location" or "security" submenu, in most cases.

Classified Information

The Department of Defence deals with extremely sensitive and highly classified information and the security of this information is of utmost importance. Cadets and Adult Members should NOT have access to any classified in information. If you or your members are presented with classified information, indicated by the markers, PROTECTED, SECRET or TOP SECRET, at the top of the page report it to your commander or manager immediately.

ADF Cadets members do on occasion have access to sensitive information, such as incident reports, personal contact details or medical information. This information should be stored in the correct manner, be treated as confidential and only disclosed when others are *required* to know.

Refer to the Youth Policy Manual Glossary on www.defenceyouth.gov.au for definitions of the terms used.

Protective Security Measures - Physical

Physical security measures provide a safe and secure environment for personnel and visitors. They include, but are not limited to:

- Barriers that deter detect and delay unauthorised entry such as fences and access controls
- Alarm systems
- Keys and combinations
- Security rooms and containers

Visitors and Visitor Escort Responsibilities

A visitor is someone who does not have a Defence-issued pass. Before gaining entry to any part of a Defence base or establishment that is NOT public access, individuals must be positively identified with photo ID. Cadets and Adult Members are NOT to sponsor or escort visitors. The sponsor and escorting officer on private Defence sites must be a Department of Defence employee (either Australian Public Service or ADF).

However cadets and adult members are responsible for reporting visitors who do not follow security protocol to their supervisor, manager or commander. This includes visitors who:

- Do not wear or display a visitor pass clearly
- Are not accompanied by an escort officer
- Attempt to gain entry into classified or controlled areas without approval

Security incidents

Any event that effects security, or that breaches security policy or requirements, is considered a security incident. Whether deliberate or accidental, security incidents are usually the result of failing to follow appropriate protocols. Recording security incidents is important to:

1. Ensure Defence information is secure and accessible only by those with a need to know
2. Prevent the same incident happening again
3. Identify trends in security incidents
4. Remind people to follow security protocols and measures

It is important to report security incidents when they happen so they can be managed and measures taken to ensure that it does not happen again. Incident reporting also enables gaps in security processes to be identified and addressed.

Security incidents are most easily managed and resolved when they are reported immediately. It is inappropriate to hide security incidents or attempt to deal with them internally, as they may have far more serious consequences than you expect.

To report a security incident either from yourself or a member of your cadet unit, inform your Defence commander. They will progress the incident reporting if required through the necessary reporting procedures of your cadet organisation.

SAFEBASE Alert System

SAFEBASE is the Protective Security Alert System used by Defence to match security measures with assessed threat levels. There are five levels which are applied to Defence bases:

ALPHA	BRAVO	CHARLIE	DELTA	ECHO
• minimum level of security • no specific threat	• medium level of security • possibility of heightened threat	• medium level of security • specific threat action likely	• high level of security • substantial threat to Defence imminent	• extreme level of security • threat about to occur or is occuring

The SAFEBASE level and the corresponding security measures applied may vary between Defence sites. The current SAFEBASE alert levels are sign-posted at the entry to Defence buildings and establishments. Each SAFEBASE alert level has specific responses and procedures that are unique to each site. Ask your manager or commander for details on the SAFEBASE level requirements for your site/unit.

You are responsible to ensure your cadets and adult members are aware of the specific SAFEBASE measures in force at your base, unit or facility. If the SAFEBASE level is changed your manager/commander will inform you and advise you on any necessary actions to be taken.