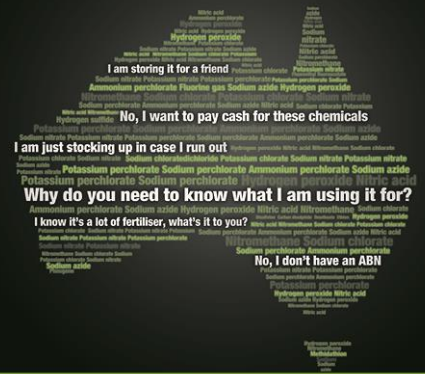
National Code of Practice for Chemicals of Security Concern



Prevent your business from becoming a target for terrorists

Terrorists can target workplaces that deal with chemicals of security concern. They may use a trusted insider—or become one—to gain access to chemicals that they can use for terrorist activities.

A 'trusted insider' is anyone who has been given access to a business's systems and physical premises. This includes past and current employees, contractors and visitors. Businesses should make sure that employees can be trusted with chemicals of security concern.

Key points

- Trusted insiders may deliberately or unknowingly help others to obtain chemicals of security concern for terrorist purposes.
- Insider threats can be difficult to predict or detect. On their own, indicators of suspicious activity may not warrant action, but together they could indicate a threat.
- Reduce the risk by making sure your business has a strong security culture and strong security programs in place. Plan your security measures carefully using the National Code of Practice for Chemicals of Security Concern and test them regularly.
- If you suspect a trusted insider in your organisation is a threat, contact the National Security Hotline on 1800 123 400.

The insider threat

Insiders can knowingly or unknowingly help others to act maliciously.

Insiders can pose a deliberate threat—using their access to premises or information systems for malicious purposes. This could include providing keys, pass cards and ID tags; disabling security devices such as cameras, sensors, locks or doors; or providing maps or schematics of facilities.

The 2004 Madrid bombings are a real-life example of insiders using information and equipment to act maliciously. One of the perpetrators stole the explosives used in the attack and the vehicles used to transport the explosives from a mining company where he worked.

Insiders can also pose an unintentional threat—helping someone to access physical facilities or information systems without realising that what they are passing on may hold significant value and may be used for malicious purposes. This often happens when someone lacks security awareness or fails to follow correct security protocol. You should provide appropriate and regular personnel security awareness training to your employees.

What to look out for

Insider threats can be difficult to predict or detect but there are several indicators to look out for:

- An employee who accesses (or attempts to access) restricted areas or information outside their area of responsibility.
- A substantial change of behaviour or circumstances in an employee—for example, they begin associating with people who hold extremist views or they suddenly become quiet or secretive. Individuals suffering from addiction or financial problems may act maliciously for financial gain, or become a target for blackmail.
- An employee who works odd hours in an attempt to be left alone in a facility.
- Unexplained or excessive copying of corporate information.
- Anyone taking video, photos, diagrams or notes of security information or access points.
- An employee with unexplained affluence—this could indicate they are receiving money or gifts in exchange for information
- Repeated breaches of your business's security arrangements.
- Theft of chemicals or items that could compromise facility security, such as uniforms, identification, blueprints, or access keys or cards.
- An employee who receives, transfers or delivers items without legitimate reason, necessary identification or authorisation.
- A pattern of losses or irregularities in inventory records—this could indicate that chemicals have been misdirected or are missing.

On their own these indicators may not necessarily warrant action, but together they could indicate a threat.

How to reduce the risk

Security awareness and training is a critical part of reducing insider threats. There are several practical steps you can take.

Before employment

- Implement a standard process for vetting new employees. Base the level of vetting on the type of information and facilities that they would have access to. This process could include criminal record and background checks where appropriate.
- Check a potential employee's identity, qualifications, work experience and references. You can do this by:
  - Asking to see identification (driver's license, passport)
  - Contacting their previous employer(s)
  - Contacting their educational institution(s)

  Follow up all inconsistencies or gaps.

During employment

- Ensure appropriate physical access controls are in place, for example ID tags, pass cards, key pads, locks and passwords.
- Implement appropriate security measures from the National Code of Practice for Chemicals of Security Concern.
- Make sure there are appropriate personnel access controls in place—only provide access to chemicals of security concern to people who have a legitimate need to access them.
- Develop staff security awareness with on-going training. Make sure staff realise the chemical security risks facing the business.
- Educate staff (both during induction and throughout their employment) on the potential misuse of the chemicals your business handles.
- Provide clear instructions on how staff can report suspicious activity—and encourage them to do so. Remind staff they can also contact the National Security Hotline on 1800 123 400.
- Refer staff to the guidance materials on the Chemical Security website: www.nationalsecurity.gov.au/chemicalsecurity.

After employment

- Recognise ex-employees may still pose a threat.
- Revoke access controls such as keys, passwords and swipe cards immediately.
- Hold exit interviews with staff and give them an opportunity to give confidential feedback on security concerns about the workplace, procedures or colleagues.

More information

The ASIO Business Liaison Unit connects Australian businesses with the Australian intelligence community.

The ASIO Business Liaison Unit is a direct point of contact into the intelligence community. They produce a large range of reports and products covering topics such as the security environment, terrorist incidents, threats to industry sectors, issue motivated groups, information security, security risk management, terrorist tactics and methodology, and country security snapshots.

You access this information through a secure website—to apply, go to the ASIO Business Liaison Unit website: http://www.blu.asio.gov.au

The Australian Federal Police can also help manage personnel security risks and conduct national criminal history checks. Visit the Australian Federal Police website for more information: www.afp.gov.au

More information on chemical security, including the national code of practice for chemicals of security concern, is available on the Chemical Security website: www.nationalsecurity.gov.au/chemicalsecurity.