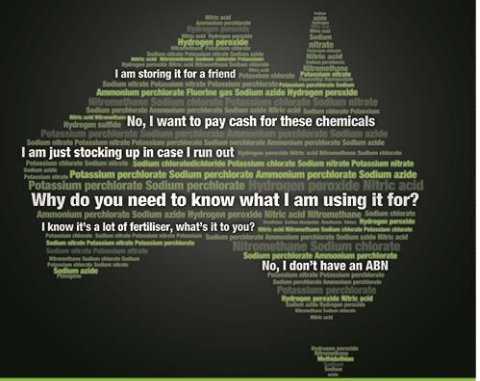
Understanding the National Code of Practice for Chemicals of Security Concern Guide



Key points

Terrorists can use some of the chemicals found in everyday products like hair dyes, fertilisers and water purifiers to poison people or make bombs.

The government has identified 96 chemicals that terrorists could use in this way. These are known as 'chemicals of security concern'.

Of the 96 chemicals, 15 are considered particularly high-risk because they can be used to make bombs or toxic weapons. You might sell, transport or use products containing these high-risk chemicals in your workplace. You need to have good security measures in place to make sure terrorists cannot access them.

The voluntary National Code of Practice for Chemicals of Security Concern provides advice for workplaces that handle the 15 high-risk chemicals. It contains practical security tips including:

- how to make sure the people in your workplace can be trusted with chemicals of security concern
- how to keep your chemicals physically secure
- how to detect and report suspicious behaviour to the National Security Hotline
- where to go for more information.

The code also has a security compliance checklist that you can use to figure out whether there are any security gaps in your workplace.

The best way you can stop terrorists from getting your chemicals is to have good security measures in place and to regularly assess your workplace security environment.

Make security a normal part of your business. Not only will you protect your chemicals from being stolen, you will also help keep Australia safe from terrorism.

Remember, if you see or hear anything that doesn't seem right, report it to the National Security Hotline on 1800 123 400. Every piece of information helps and you can remain

About this document

This document is a guide to help you understand the National Code of Practice for Chemicals of Security Concern and how it can help you to protect and secure your chemicals. You can find out more by reading the National Code of Practice for Chemicals of Security Concern. There is a copy of the code, and other resources, on the chemical security website: www.nationalsecurity.gov.au/chemicalsecurity.

Applying the code

Does your business hold high-risk chemicals of security concern?

The table below lists the 15 high-risk chemicals covered by the code. It's a good idea to check whether your business deals with any of these chemicals before you apply the code in your workplace. If you manufacture, store, transport or sell (including online) any of the chemicals in the table below, then the code applies to you. The code also applies to businesses involved in the disposal and recycling of chemical waste or recovery of used chemicals.

You can find out whether your products contain these chemicals by:

- checking the labels of your products
- checking the material safety data sheet, safety data sheet or product safety data sheet (or similar documentation) that your product supplier gave you
- contacting your product supplier for more information.

Chemical	**Concentration/form**	**Typical uses in Australia**
Aluminium phosphide	Any concentration	Mixed function pesticide used in agriculture.
Ammonium perchlorate	Ammonium perchlorate where it is in a water-based solution and the ammonium perchlorate is at a concentration of at least **10%**, and Ammonium perchlorate (in any other form) at a concentration of **65%** or above.	Fireworks and explosives, rocketry, laboratory and diagnostic reagent.
Chlorine	Gas only	Water treatment, mining, calibration gas, chemical manufacture, scientific research, fuel gas mixture.
Hydrogen peroxide	Hydrogen peroxide in a water-based solution at any concentration, and Hydrogen peroxide (in any other form including a liquid mixture) where the hydrogen peroxide is at a concentration of **15%** or above.	Paper and pulp bleaching, laundry, food and beverage, cleaning, dairy, hair and beauty, mining, pool and spa, pharmaceuticals, water treatment, cleaning.
Nitric acid	Nitric acid at a concentration of **30%** or above.	Mining, metal processing and treatment, food and beverage, dairy industry.
Nitromethane	Nitromethane at a concentration of **10%** or above.	Pharmaceuticals, analytical laboratories, as a racing fuel in high performance racing and in hobby shops as a fuel component in radio-controlled models.

Chemical	Concentration/form	Typical uses in Australia
Potassium chlorate	Potassium chlorate where it is in a water-based solution and the potassium chlorate makes up at least **10%** of that solution, and Potassium chlorate (in any other form) at a concentration of **65%** or above.	Fireworks and explosives, laboratory and diagnostic reagent.
Potassium cyanide	Any concentration	Mining, agriculture, scientific research, electroplating, cleaning jewellery
Potassium nitrate	Potassium nitrate where it is in a water-based solution and the potassium nitrate makes up at least **10%** of that solution, and Potassium nitrate (in any other form) at a concentration of **65%** or above.	Fertilisers, fireworks and rocketry, food preservation.
Potassium perchlorate	Potassium perchlorate where it is in a water-based solution and the potassium perchlorate makes up at least **10%** of the solution, and Potassium perchlorate (in any other form) at a concentration of **65%** or above.	Fireworks and explosives, smelting, a laboratory and diagnostic reagent.
Sodium azide	Sodium azide at a concentration of **95%** or above.	Smelting, a biocide in hospitals and laboratories, dairy industry.
Sodium chlorate	Sodium chlorate where it is in a water-based solution and the sodium chlorate is at a concentration of **10%** or above, and Sodium chlorate (in any other form) at a concentration of **65%** or above.	Mining, metal treatment, paper production, food chemical, laboratory and diagnostic reagent.
Sodium cyanide	Any concentration	Insecticides, gold extraction, ore flotation, electroplating, used in metal cleaning baths, metal hardening.

Chemical	Concentration/form	Typical uses in Australia
Sodium nitrate	Sodium nitrate where it is in a water-based solution and the sodium nitrate is at a concentration of **10%** or above, and Sodium nitrate (in any other form) at a concentration of **65%** or above.	Fertilisers, pyrotechnics, food preservative, rocket propellant.
Sodium perchlorate	Sodium perchlorate where it is in a water-based solution and the sodium perchlorate is at a concentration of **10%** or above, and Sodium perchlorate (in any other form) at a concentration of **65%** or above.	Mining, smelting, laboratory and diagnostic reagent.

Certain chemical combinations can be more risky than others. For example, a product that contains a high-risk chemical that can easily be extracted is a greater a security risk than a product where the high-risk chemical is harder to extract. You should have more security measures in place for higher-risk products.

If your business deals with one or more of the chemicals in the table above, you should use the practical tips and security measures in the code to find out what your security risks are and take steps to reduce them.

Managing security risks

Managing security risks is a normal part of good business practice. It should be part of your business culture and your day-to-day operations.

By having good security risk management in your business, you will be able to:

- identify and assess security risks
- make informed decisions about the security of your chemicals
- choose cost-effective ways to increase security
- create and maintain a good security culture.

This will lower the risk of your chemicals being used for terrorist purposes.

Assessing your security risk

The first thing you should do is carry out a workplace security assessment. You can do this by reviewing your current processes to work out how and where chemicals could find their way into terrorists' hands.

Look at how well your current systems and security procedures are working and whether they could be improved. For example, you could look at the following types of security in your workplace:

- physical security (eg storage facilities, locks and gates)

- personnel security (eg background checking your employees and contractors)
- information security (eg making sure unauthorised people cannot access your computer networks)
- policies and procedures (eg having good workplace security policies in place).

Steps you can take to reduce your security risks are outlined in section 3 of this document. Looking at these steps will help you decide whether your existing procedures are good enough, and if not, what you could do to make them better. Remember, your current arrangements may already be enough to manage the risk of terrorists taking chemicals from your business. For more detail, you can look at the 'security measures' section of the code.

To help you work out whether you have some security gaps in your workplace that a terrorist could take advantage of, read the following examples of common ways terrorists can get chemicals:

1. **Theft**— where chemicals are stolen from your workplace by an employee or an outsider.
2. **Diversion**— where chemicals are diverted from your workplace through deception. This can include the following tactics:
    - *Hijacking*—for example, an employee or customer places an order that requires the chemicals to be transported and then steals the chemicals while they are in transit.
    - *Fraud*—for example, an employee or customer sets up a fake company, places an order, collects the chemicals and then closes the company or disappears once the order is delivered.
    - *Coercion*—for example, an existing customer or employee is forced or bribed into ordering or diverting chemicals for terrorists.
    - *Business as usual*—for example, an order is placed by someone pretending to be a legitimate customer, but they are actually going to use those chemicals for terrorist acts.
    - *Hacking*—for example, your network or computer system is hacked and a delivery is scheduled and hidden. The delivery route may also be changed in this way.

You should consider scenarios like those listed above when you are doing your security risk assessment.

The following websites have more information to help you assess your security.

1. The chemical security website— www.nationalsecurity.gov.au/chemicalsecurity contains sector-specific guidance, risk assessment advice and training materials.
2. The ASIO Business Liaison Unit website— www.asio.blu.gov.au includes information to help businesses better understand the national security environment.
3. The National Security website— www.nationalsecurity.gov.au includes information about Australia's national security environment.
4. The Standards Australia website— www.standards.org.au contains security management guidelines:
    - HB 158-2010 Delivering assurance based on ISO 31000:2009 Risk Management— Principles and Guidelines.
    - HB 167:2007 Security Risk Management.

Reducing your risk

You know your business better than anyone else, and that's why it is important for you to think about the risks in your own workplace and to take appropriate, cost-effective steps to reduce your risks.

The security measures you use should support and complement each other. For examples of security measures you can use in your workplace, refer to the 'Security measures' section of the code.

You do not have to use all of the security measures in the code unless you decide your workplace needs them. For example, it may be too costly or impractical for you to do background checks on all of your employees. Instead, you may decide to reduce your chemical security risk by only allowing senior staff to access your chemicals and training staff to identify suspicious behaviour. The steps you take may just be improvements on the security procedures you already have in place.

Background checks for employees and contractors

Someone with access to inside knowledge of your organisation (in relation to your security, systems or facilities) is known as 'trusted insider'. A trusted insider could take advantage of this knowledge to cause harm, for example by stealing (or helping terrorists to steal) your chemicals—this is known as an insider threat.

It could be someone who started working at your workplace with the intention of doing harm. Or someone who is already working at your workplace who is convinced or forced by others to do harm. It could also be someone who just decides to do harm during their time at your workplace. This is not limited to new employees or contractors—it can also be permanent staff employed in a workplace for several years. They may abuse their access to your resources or facilities or take advantage of security loopholes.

Insider threat activities can include things such as:

- unauthorised disclosure of information
- letting unauthorised people access the premises
- theft.

Whatever the motivation behind it, insider threat activities can cause harm, disruption and embarrassment to your business.

More information on the insider threat is available on the chemical security website—www.nationalsecurity.gov.au/chemicalsecurity or through ASIO's Business Liaison Unit website—www.blu.asio.gov.au

The code suggests four ways you can check the trustworthiness of your employees and contractors to reduce the insider threat.

These are:

- general background checking
- identity checks
- previous employment checks
- criminal record checking.

When you are deciding which methods to use and what actions to take when you receive the results of an employee or contractor check, you should consider the requirements of the job. For example, employees who have unsupervised access to chemicals as part of their normal job will require more security checking than administrative staff or employees who have limited access to chemicals.

If you are concerned, you should seek legal advice on your decision and process.

General background checking

One way to help protect your workplace against insider threats is by doing general background checks on prospective employees or contractors to make sure that they are who they say they are. Background

checks can also determine someone's trustworthiness and how suited they are to the job. Background checks are a good way to decide whether the person could be trusted in a job that gives them access to your business, systems and resources—including high-risk chemicals.

You can repeat the background checks on existing employees and contractors at regular intervals, and also when a person is being transferred or promoted to a work area with access to high-risk chemicals.

Background checking may be hard if the person you wish to check is a family member or a friend, but you should still make sure you have enough knowledge about them to decide whether you can trust them with your businesses, systems or high-risk chemicals.

The results of a background check will help you decide whether the person is suitable to perform the requirements of the job. When making your decision, you should consider any security risks involved with the job.

Identity checks

You can also check the identity of a prospective employee or contractor. This process involves checking their full name, date of birth and residential address by looking at proof on an official document. Official documents could include a driver's licence, 18+ card, passport or, if the person is aged under 18, a school reference or report.

Details of how to check the identity of a potential employee or contractor can be found in the following publications:

- Australian Standard (AS) 4811-2006 Employment Screening
- HB 323-2007 Employment Screening Handbook.

You can purchase these publications through the SAI Global website (www.saiglobal.com).

Previous employment checks

You can check a prospective employee or contractor's previous work history by looking at their CV, résumé or similar document. Look out for any unexplained gaps or anything unusual. This may give you an indication of whether the person is trustworthy to employ.

You could also contact the person's previous employers or referees for a reference. This includes contacting a group training officer if the prospective employee or contractor is being engaged under a group training scheme or similar.

If there is a gap or abnormality in any of the information the prospective employee has given you, you should ask them to explain it. If the person seems suspicious, you can report your concerns to the National Security Hotline on 1800 123 400.

Criminal record checking

You should only check a person's criminal history where there is a clear security risk related to the essential requirements of the job, for example if the employee has access to chemicals without supervision. It is unlikely that a criminal record check will be needed if the employee only has access to chemicals when they are with another employee or supervisor.

The Australian Federal Police can provide National Police Checks for:

- residents of the ACT, Jervis Bay Territory and external Commonwealth territories
- people seeking employment with the Australian Government
- people requiring a check under Commonwealth legislation
- Australian immigration purposes

- applicants that live overseas
- overseas employment
- overseas adoption
- visa applications for overseas travel.

Find out more on the Australian Federal Police website at www.afp.gov.au

For criminal record checks in other states, you should contact your state or territory police service:

- New South Wales Police : www.police.nsw.gov.au
- Northern Territory Police: www.police.nt.gov.au
- Queensland Police: www.police.qld.gov.au
- Tasmania Police: www.police.tas.gov.au
- Victoria Police: www.police.vic.gov.au
- South Australia Police: www.police.sa.gov.au
- Western Australia Police: www.police.wa.gov.au

To avoid discrimination, an employer should only refuse to employ a person if the information discovered, during a background check or criminal record check, means that the employee is unable to perform the requirements of the job. This requirement is contained in federal, state and territory laws. Each person's ability to fulfil the inherent requirements of the job should be assessed on a case by case basis. The document, *On the record: guidelines for the prevention of discrimination in employment on the basis of criminal record* provides more guidance. You can access it on the Australian Human Rights Commission website. Go to www.humanrights.gov.au and click the 'publications' page. Use the search function on this page to find the document you wish to read.

You can also visit the Fair Work Ombudsman website— www.fairwork.gov.au for information about workplace relations.

Legal obligations

There are several legal issues associated with background checking. For example, if you are storing someone's personal information, you need to be mindful of privacy law requirements.

If you have any concerns or questions, you should seek your own legal advice to make sure that your processes comply with any legal requirements.

Legal issues could include:

- discrimination
- privacy
- workplace health and safety.

Update contact details

At least once a year you could ask employees who work with high-risk chemicals or security systems to update their personal details in your system. This is particularly important if their job requires identification or notification of changes in personal details.

Personnel security awareness

Educate employees and contractors

Employees and contractors see what occurs around your workplace and are well-placed to notice when something doesn't seem right. By providing them with training on how to identify and report suspicious behaviour and activities, you can improve the security culture of your workplace. When your workplace has a good security culture, it means that security loopholes or breaches are more likely to be reported. This will allow you to deal with the matter before it causes damage to your business.

You should teach your employees and contractors about security issues such as:

- the risk of common chemical products in your workplace being used to make homemade explosives or toxic devices
- how to identify products in your workplace that contain high-risk chemicals
- the legitimate uses for products containing high-risk chemicals, including the recommended quantities of the products
- 'knowing your customer'— for example, ways to figure out why the customer wants the chemical product and ways to advise them on the right quantities to use
- indicators of insider threat activities— for example a co-worker working odd hours in an attempt to be left alone in a workplace, or accessing restricted areas or information outside their normal responsibilities
- inventory control mechanisms and how to detect and prevent theft or diversion of chemicals
- indicators of suspicious behaviour
- the importance of reporting anything suspicious to the National Security Hotline on 1800 123 400.

You can find training and awareness raising resources on the chemical security website— www.nationalsecurity.gov.au/chemicalsecurity.

You can also contact chemical.security@ag.gov.au if you require further information.

Inventory control

You can work out whether chemicals have gone missing by regularly monitoring your stock inventory.

Report any unexplained losses to the National Security Hotline on 1800 123 400 and the police.

A good inventory control system is one that helps you to:

- identify products containing high-risk chemicals of security concern in relevant concentrations and forms
- pinpoint the physical location of each product container at any time
- identify the number of containers or the total weight of the product at the start of a particular time period
- identify the number of containers and/or the total weight of the product at the end of a particular time frame.

It is up to you to determine how often you check and reconcile your stock, taking into account your individual circumstances.

As a guide, your system should help you to address one or more of the following suspicious activities:

Suspicious activity	**What it could mean**	**Next steps**
A customer's identity is unclear, or the customer's business is newly registered or they have recently, or regularly, changed their company name.	The customer may be purposely trying to avoid being identified, as they may be using chemicals for terrorist purposes.	Check their telephone, trade and ABN (Australian Business Number) records. You can check an ABN by visiting the Australian Business Register's website. Go to www.abr.gov.au and click the 'ABN lookup' link. Use the search function on this page to check an ABN. You could also check with the relevant industry organisation for their business. You could type the customer's name or business name into Google to check whether they have a business website or an online profile. If the customer does not provide proper identification details and you have no way of working this out from the information they have provided, you may wish to report this suspicious transaction to the National Security Hotline.
The type of business that is buying the goods doesn't match with the type of goods they are buying (for example, a youth outreach organisation purchasing a large volume of hydrogen peroxide).	The customer may be using the business as a cover for their terrorist activities.	You can research their business online or through the relevant industry organisation. That way you can detect whether something does not seem right. If it doesn't feel right, you can report it to the National Security Hotline.

Suspicious activity	What it could mean	Next steps
The customer does not state how they are going to use the product/chemical. The customer says they are going to use the chemical product in a way that is different from its normal purpose (for example, John Smith wants purchase 5kg bags of a chemical product online and states that he will be using it for cosmetics when that product is normally used as a fertiliser).	The customer may be lying or avoiding letting you know what they are using the chemicals for. This may be to cover up the fact that they will be using the chemicals for terrorist activities.	You could ensure that your security system asks for each customer to report the reason they are purchasing your chemical products. That way you will be able to detect when something does not seem right.
The customer or transaction seems to involve an agent.	The customer may be trying to avoid being identified, as they do not wish to have the purchase traced back to them. This may be because they are involved in terrorist activities.	You can check whether the person ordering chemicals from you online is the same person that is receiving the chemicals. You could do this by checking whether the delivery address matches up with the customer's address.
The customer doesn't ask for or turns down the assistance of a technical expert or training assistance when this is generally considered normal for people using the product.	This may mean that the customer does not intend to use the product for its normal use, and instead is going to use it for terrorist purposes.	You could include a 'check box' in your online ordering system, which asks whether the customer would like technical assistance with their purchase. That way, if they do not request technical assistance, you may have a reason to think that this transaction is suspicious.
The customer orders an unusually large volume of the product.	This may mean that the customer is planning to use the product to create a homemade explosive or toxic device for terrorist purposes.	You could set up your online system to automatically flag any purchases over a certain amount.

Suspicious activity	What it could mean	Next steps
The customer makes several repeated purchases.	The customer could be stockpiling chemicals to make explosives.	You could set up your online system to automatically detect repeated purchases from the same customer or account, so that you can have a record of whether someone is purchasing a suspicious amount of chemicals.
The customer contacts you asking to pay in cash, rather than by card, direct debit or cheque.	The customer may be trying to avoid being traced.	You should only offer direct debit or credit card payment for online sales. These types of transactions are traced more easily than cash.
The customer makes an unusual request for urgent delivery, or other unusual requests regarding the shipment/delivery location or route.	The customer may be ordering chemicals for a terrorist activity planned on a certain date or at a certain place.	Your security system could include a requirement for the customer to provide a reason for urgent delivery. If their answer seems unusual, or they do not answer, you may decide that this transaction is suspicious and should be reported to the National Security Hotline.
The customer orders commercial (large) quantities of a product but asks them to be delivered to a residential address.	The customer may be ordering chemicals to make a homemade explosive or toxic device for a terrorist act.	You should check the customer's delivery address to see whether it is a residential address or a business address. That way you will be able to detect whether the delivery address seems suspicious.
The customer asks for a delivery to a PO box, or an area that does not match the nature of the products (for example, a customer asks for agricultural chemicals to be delivered to an urban area).	The customer may be trying to avoid being identified. This may be because they are going to use the chemicals for terrorist purposes.	You should check the customer's delivery address. That way you will be able to detect whether the delivery address seems suspicious.

Suspicious activity	What it could mean	Next steps
A business customer is communicating via email using a generic email account (such as Hotmail, gmail or similar) rather than a business email account.	The customer may be pretending to operate a legitimate business. This may be to cover up terrorist activities.	You may be able to include a detection mechanism in your security system for generic email addresses. If your customer is using a generic email address, and there are other signs that indicate the transaction may be suspicious, you should report this to the National Security Hotline.
The business customer's order contains spelling errors and simple mistakes.	The customer may be pretending to operate a legitimate business. This may be to cover up terrorist activities.	Your system may be able to flag simple mistakes and provide a way for you to follow the customer up for clarification or more information. If you still feel the transaction is suspicious, you should report your concerns to the National Security Hotline.

The table above outlines just some of the behaviours that could be suspicious in the online sales environment. The main thing is to trust your instincts. If something doesn't seem quite right, report your suspicions to the National Security Hotline on 1800 123 400.

Other tips

- make it easy for your staff to let senior management know about any suspicious behaviour - senior staff review the sale and decide whether to report it to the National Security Hotline and whether to refuse the sale
- train your staff about suspicious behaviour— make sure that all sales staff, including those who process email sales, know the signs to look out for.

Transporting chemicals

Chemicals can be hijacked in transit. Businesses that transport chemicals to and from their business, or between different business premises, need to make sure they have good security measures in place.

These are some of the things you could do to reduce your security risk:

- make sure that relevant chemical products are locked away at all times during transit
- make sure vehicles are not left unattended unless they are in a secure site
- have a system in place to monitor the location of products during transit
- have accurate weighing procedures or other methods for checking chemical stock at loading and unloading points, to make sure that the amount delivered has not changed
- confirm that each load is delivered with all seals and locks intact
- only deliver chemicals or products to the nominated recipient, and verify their identity.

If the chemicals you are transporting fall under the Australian Dangerous Goods Code, that code overrides the National Code of Practice for Chemicals of Security Concern if there is any inconsistency.

You can find the Australian Dangerous Goods Code on the Department of Infrastructure and Regional Development website. Go to www.infrastructure.gov.au and click the 'transport' tab. Click the 'transport in Australia' link and then click the 'dangerous goods' link. On this page you can find the most recent edition of the Australian Dangerous Goods code.

Waste disposal, recycling and resource recovery

Terrorists may be interested in stealing, diverting or hijacking chemicals even when the chemicals are being disposed as waste, recycled or recovered for other uses. Terrorists could be interested in getting hold of your chemicals at any stage in the process including while they are in transit or in storage. Businesses involved in chemical waste management, recycling or recovery should use the practical tips and security measures in the code to determine what your security risks are and to take steps to reduce them.

If you already comply with the National Environment Protection Measures, or specific state or territory regulations for the management and transport of waste, it is likely you will already have effective measures in place.

Businesses involved in disposal, recycling or recovery activities will handle a wide range of chemicals and in different forms. These could include pure chemicals, spent chemicals or even complex mixtures. In some cases, it might be hard to know if you are dealing with a high-risk chemical (listed on pages 3-5 of this document). If you are unsure, you should find out by asking the original owner of the chemical waste.

Certain chemical mixture can carry a higher risk than others, and you should consider this as part of managing your security risks. While a complex mixture of several chemicals may make it difficult for a high-risk chemical to be extracted, the mixture itself can be significantly toxic and therefore be of interest to terrorists.

Privacy considerations

Personal information is any information that identifies, or could reasonably be used to identify a person. There are some obvious examples of personal information, like a person's name and address. It can also include medical records, bank account details, photos, videos, and even information about what an individual likes, their opinions and where they work.

By recording the details of someone acting suspicious, you could be collecting a customer's personal information. There are legal requirements around how you collect, store and use someone's personal information.

Make sure that the personal information you collect is protected from unauthorised access, misuse or loss. You should consider:

- training staff in privacy procedures
- keeping hard copy files in properly secured cabinets
- limiting access to personal information to only authorised staff members
- regularly monitoring your information handling practices to ensure they are secure.

The Office of the Australian Information Commissioner website contains several useful privacy resources, including a factsheet outlining ten steps that businesses can take to protect other people's personal information. Go to www.oaic.gov.au click the 'agencies and resources tab' and then click the 'business resources' link.