SOUTH AUSTRALIA POLICE
KEEPING SA SAFE

PREVENTING CRIME

BUSINESS SECURITY
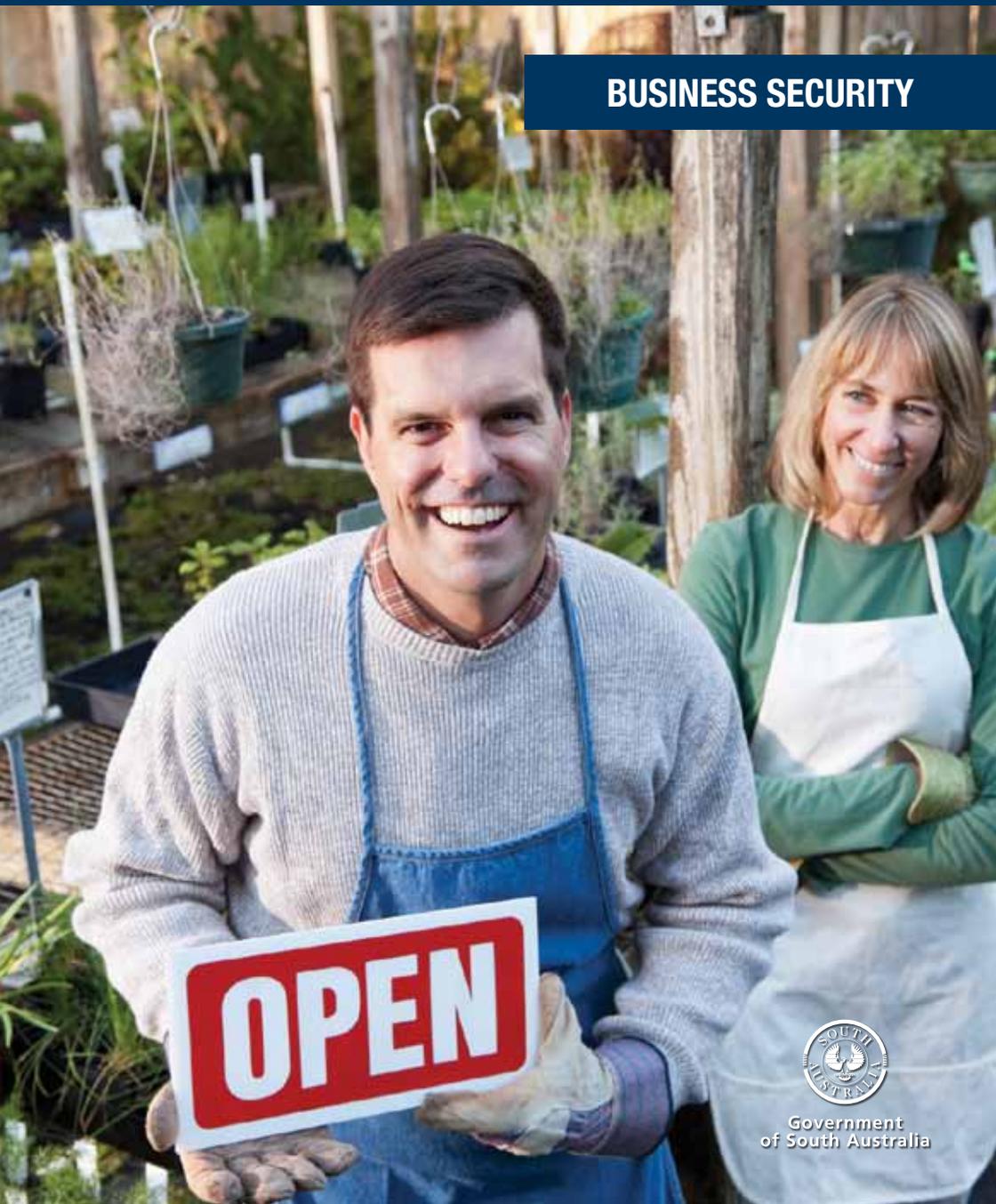
Government
of South Australia

INDEX

Dear Business Owner,

South Australia Police (SAPOL) is committed to working in partnership with the community to prevent crime and reduce the fear of crime to ensure that South Australia is a safe place to live, visit and do business.

This book has been developed to provide you with practical tips to improve the security of your business. We encourage you to:

• read this book and share the information with your staff
• take the time to conduct your own Business Security Assessment and apply the suggested treatments where necessary
• place the 'No cash' sticker in a prominent position at the entry point to the premises
• place the 'Height' sticker either near the entry or near the counter area (use a tape measure to ensure all heights are accurate)
• place the 'Keep cash low' sticker near your cash points.

For further assistance please contact your Local Service Area Crime Prevention Section or visit www.police.sa.gov.au

For a safer
South Australia
everyone must accept
responsibility for
crime prevention

RETAIL THEFT PREVENTION

- Clearly display warning signs regarding the consequences of theft and the security measures in place at your business.
- Staff should have clear line of sight within the business. If blind spots occur, install convex mirrors or mirror tiles or CCTV cameras. Ensure any reflective devices do not allow vision of business practices by visitors.
- Limit the number of entry and exit points to your business.
- Ideally, cash registers should be located close to exit points of the business and should be protected to prevent easy removal of money by offenders, such as elevating the cash register or counter area. This also improves the view for staff.
- When showing valuable goods to a customer, avoid placing more than one item on the counter at a time, particularly small items. It can lead to theft, confusion and/or fraudulent behaviour.
- Stock and shelves should be neatly stacked and price tags should be properly secured to goods.
- Use price tags that cannot easily be removed or altered.
- Check the correct price of an item if a ticket is mutilated, attached incorrectly, altered or missing.
- Give customers receipts for all purchases and spot check receipts at exits. Check expensive items as offenders can be very brazen by walking out the door with goods not paid for.

- Check the number of garments taken in and out of fitting rooms and remove all surplus clothing from fitting rooms after each customer.
- Alternate the hooks on clothes racks to prevent snatch and grab offences.
- Do not have 'specials' tables at the front or outside the business unless permanently staffed.
- If the merchandise you are selling comes in pairs, only display one and advertise this fact.
- Display 'dummy' or 'disabled' goods when practicable (e.g. CD covers, DVD's, computer game boxes, etc).
- Where possible, lock expensive and easily portable goods in cabinets located close to staff working areas.
- A simple but smart uniform gives staff a sense of 'belonging' and 'authority' and ensures that staff are highly visible.
- Make sure that visitors have no direct access behind counters and the public and private areas are clearly defined.

STAFF EDUCATION

Ensure all staff understand:
- procedures that are to be followed in relation to theft and bag searches, and
- what is expected of them in relation to the apprehension of a thief.

Encourage staff to:
- acknowledge all visitors when they enter the business
- pay attention to visitors who are nervous or who appear distracted
- approach people who stand around staff restricted areas, toilets, stockrooms or stairways

- be aware of people wearing loose overcoats and bulky clothing, especially in hot weather
- approach and query persons claiming to be tradespersons, particularly in unauthorised areas
- be vigilant of persons wheeling strollers or trolleys, carrying boxes or bags and other items that may assist in concealing stolen goods
- keep visitors in view at all times and escort them around the premises if necessary
- never leave cash registers unattended
- examine all packaging on products for signs of tampering as other products may be hidden inside.

DETECTION

Watch for:

- hands - they do the stealing
- visitors who do not appear to have a deliberate purpose to be inside the business
- visitors who remain in the business for lengthy periods of time, or who are sampling merchandise that does not fit their character
- visitors who appear nervous, perspire, appear agitated or won't make eye contact
- organised distractions where there are one or more (or groups of) persons attempting to commit thefts while distracting staff.

Watch for hands - they do the stealing

APPREHENSION

- Staff members have a lawful right to ask a suspected thief to return to or remain at the business. It is important that a set of procedures are put in place and that staff adhere to these procedures to maximise their safety and to ensure they act lawfully when dealing with situations of suspected theft.
- The staff member who witnesses the offence MUST be sure of:
  - having seen the goods being taken
  - where the person has placed or concealed the item/s
  - maintaining continuous observation of the person
  - that the person failed to pay for the goods
  - that the goods are in the possession of the person and haven't been dumped
  - that the person has passed the last point of payment.
- If it safe to do so, approach the person and ask them to return to the business.
- Do not directly accuse the person of theft as this may aggravate the situation.
- Do not touch or search the person.
- Call police on 131 444 and wait for their attendance.
- If it is unsafe to approach the person or they refuse to return to the business, call police.

Remember, safety is paramount.

CREDIT CARDS

- Be alert for customers that act in an unusual manner, who may:
  - appear to be in a hurry, nervous, blushing, talking hesitantly or someone who is being overly chatty or friendly
  - make a purchase without regard to the price, quality or size
  - repeatedly returns to make additional charges
  - bring a card straight out of a pocket instead of a wallet.
- When you receive the card, look at the front and check to see if:
  - the expiry date is current
  - the name matches the person (i.e. male name for male person)
  - the card is not damaged
  - the embossing has not been altered
  - the hologram is authentic (look for quality, correctness, 3D features, change of colour).
- When you check the signature:
  - ensure the card is signed and the signature has not been altered
  - ensure the signature on the sales strip matches that on the actual card.
- If using an electronic terminal, ensure printed receipts match the printed details on the card.
- Do not return the card to the customer before the sale has been processed and the signature confirmed.
- If you have a manual imprint system, ensure carbon sheets are destroyed or returned to the customer.

- Should alterations or irregularities be found:
  - ask for additional photo identification
  - hold onto the card
  - call for authorisation.
- Contact the authorisation centre to obtain authorisation for credit card transactions where:
  - the value of the transaction is high for the business
  - the person presenting the card is suspected of not being the cardholder.

  If the transaction is not authorised:
  - hold onto the card
  - listen to the instructions given to you from the credit card authorising agency
  - call police on 131 444.
- Check that the refund limit for each EFTPOS terminal is set at an appropriate limit.
- Ensure the EFTPOS password or PIN is changed regularly and kept confidential.
- Ensure there is sufficient physical security of EFTPOS terminals.
- Ensure staff are trained to identify fraudulent credit cards, cheques and currency.

BANKING SECURITY

- Keep minimal amounts of cash at your business.
- Ensure cash is not left on premises overnight.
- Money should be counted away from customers and stored safely if banking is not possible.
- Vary times and routes when banking.
- Conceal the fact that you are carrying cash. Do not use bank identifiable bags.
- Remove or cover badges and uniforms that identify you when you are going to the bank.
- Have two staff members attend to banking where possible.
- When carrying cash, populated areas are safer than deserted areas.
- Conceal the fact that you are banking for a business.
- Shop takings should never be discussed in public.
- Use local bank services to reduce the amount of time spent carrying cash in transit.
- Ensure the time of return is known to fellow co-workers so an alarm can be raised if necessary.

CASH IN TRANSIT

- Consider using a professional, accredited cash carrying service.
- To check whether the company is licenced in South Australia, visit the Office of Consumer and Business Affairs website www.cbs.sa.gov.au/licensing/regpub and search under the licensing public register.
- Before signing a contract:
  - sight the company security licence and check the company's conditions
  - if you choose a service with convert armed guards the company must provide written authority from SAPOL Firearms Branch, stating they are licensed to carry covertly
  - all employees must hold a current South Australian firearms licence.
- Revisit the Officer of Consumer and Business Affairs at regular intervals to check for any changes on the licence conditions or status of the company.

> Vary times and routes when banking

IDENTITY CRIME

WHAT IS IDENTITY CRIME?
'Identity crime' is the use of a false identity to gain money, goods, services or other benefits and can include the following types of criminal activity:
- counterfeiting and skimming of credit cards
- the use of stolen credit cards or credit card numbers
- fraudulently obtaining money, finance, credit, benefits, pensions or entitlements
- evading the payment of taxes, levies or other debts. False identities are often created by manufacturing or forging legitimate documentation of a person's identity (living or dead), utilising stolen or fraudulently obtained personal information.

Staff need to be alert when dealing with all transactions and be alert for suspicious behaviour.

IDENTITY THEFT
Identity theft often results in fraud by a 'takeover' of the victim's existing bank accounts or by the fraudulent operation of new accounts opened in the victim's name.

Victims of identity theft may have difficulty in undoing the damage caused to their good name, reputation or credit rating. Correcting identity theft can be time consuming and frustrating for victims.

PREVENTING IDENTITY CRIME
Shred, rip up or destroy confidential personal and business documents (bank and credit card statements, all utility accounts) before disposing in a bin.

Be careful about releasing personal or business information over the phone or internet. Always know who you are dealing with and where your information is going.

Use secure transaction methods when processing credit card transactions on the phone and internet. Criminals can exploit this type of transaction using credit card numbers from innocent victims - the merchant ultimately loses out when the credit is later reversed. Contact your financial institution for more information on how to secure these transactions.

Internal business documents such as cheques and letterheads should be distinctive and include some type of security feature to deter forgery.

Use secure transaction methods when processing credit card transactions on the phone or internet

COMPUTER SECURITY

Improve your computer security by following these tips:

- portable electronic goods should be locked away when not in use
- close blinds or curtains if your computer is near a window so it is not in clear view
- use a computer security device like a 'cut resistant' steel cable to secure laptops to a fixed object
- lock internal doors/windows when the business is unattended
- if you must leave a computer in a vehicle, store it in the boot prior to your final destination and use a cable lock to secure it
- identify your computer by either engraving it, marking it with an ultra violet (UV) pen or using micro dot technology
- all property should be clearly and permanently marked with the name of your business or your Australian Business Number (ABN). Your property could also be marked with your driver's licence number prefixed by the letter 'S' for South Australia, e.g. S123456, or business name and suburb
- record model and serial numbers and keep in a safe place
- remove lockable hard drives and USB data storage, storing them in a secure place when not in use
- do not 'advertise' the purchase of a new computer or component by placing empty boxes next to the rubbish bin
- consider installing a firewall and up-to-date virus protection software
- where possible, program your computer with a password to restrict access.

STAFF EMPLOYMENT

RECRUITMENT
- All applications for employment should be carefully screened, including the sighting of original photographic identification.
- References should be checked and any unexplained gaps in past employment should be explained if suspicious.
- Consider requesting applicants to produce a national Police Check.

EMPLOYMENT
- An induction program for new employees should be conducted providing them with a clear understanding of security procedures.
- Ensure your policies are clear and explain what actions are not acceptable and liable to further action by management.
- Advise all staff of the procedures to be followed when they purchase goods from your business.
- Provide strong and consistent supervision of all staff and immediately deal with issues of concern.
- Provide ongoing security training programs to all staff and encourage employee contribution to security initiatives.
- Put procedures in place that make employee theft more difficult and which also increase the possibility of getting caught, including random bag checks and the security tagging of merchandise.
- Have an effective asset inventory control system to identify losses as they occur.
- All personal belongings should be locked away in a designated, secure area.
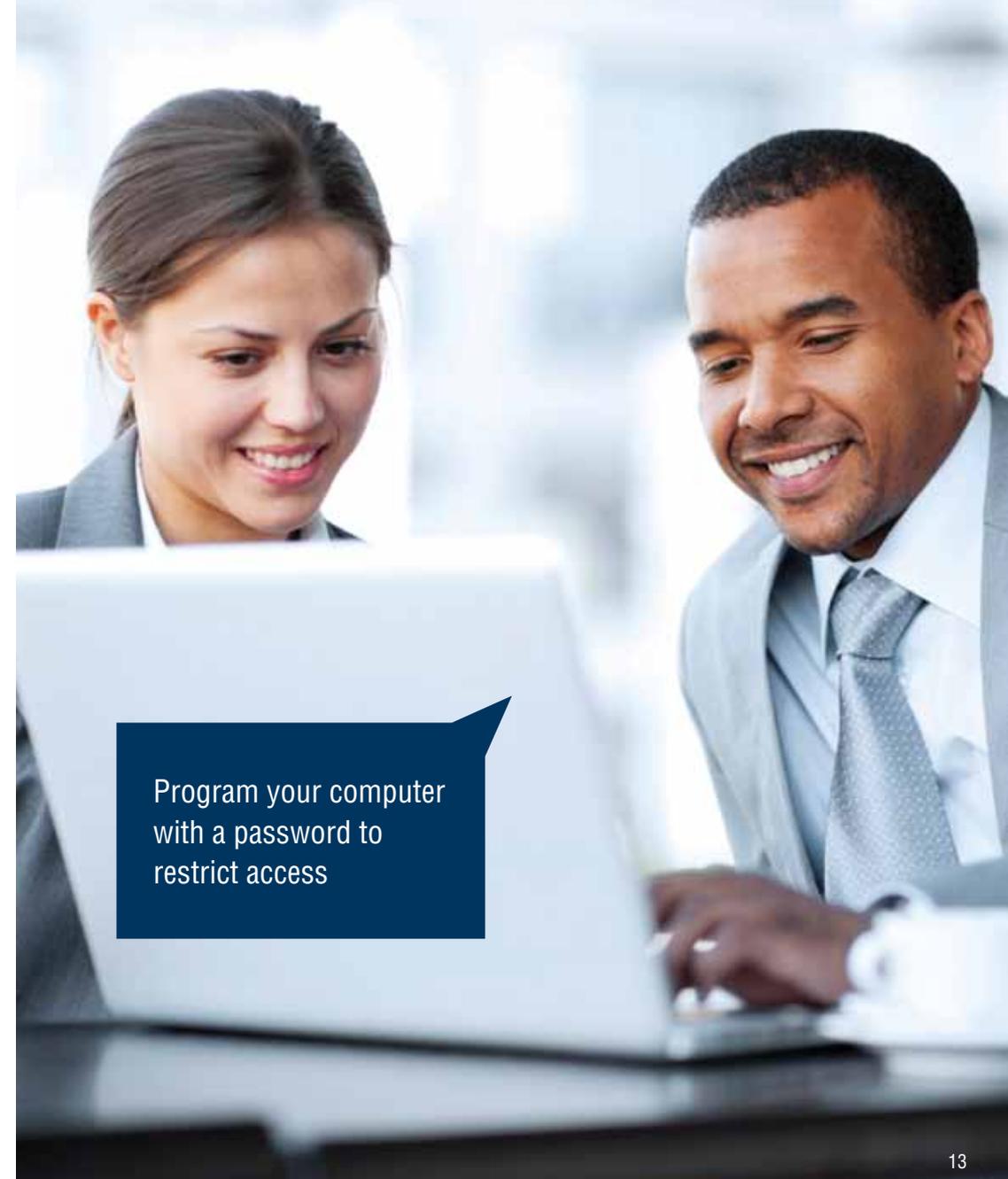
Program your computer with a password to restrict access

- Key control must be maintained at all times to ensure internal security.
- Careful checks should be made at dispatch and delivery areas to prevent falsification of records, theft and poor resource management practices.
- Ongoing issues in relation to short falls in daily takings should be investigated immediately.
- Watch for customers recognised as continually returning to the same register or customers who appear to be over friendly with the staff.
- Remember that most staff are loyal to their employers.

AGGRESSIVE CUSTOMERS

In all instances of dealing with aggressive persons, the main priority is to ensure personal safety and the safety of others. Aggressive people can be unpredictable, so encourage staff to be cautious at all times.

- Assess the situation and remain calm.
- The early stages of any confrontation are always the most dangerous. If a staff member believes their safety or the safety of other people is at risk, then the police should be contacted immediately on Triple Zero (000).
- Do not react to the customer's bad behaviour in a similar manner.
- Do not take insults personally and keep a safe distance away from the aggressive person.

- Do not enter the person's physical space as this can escalate the situation.
- Use counter areas or display stands to create distance and space.
- Staff not involved should not become an audience, but they should discreetly monitor the situation for the safety of their colleague.
- Patience is usually the best strategy. This is best achieved by listening to the person and acknowledging their problem or situation so they can vent their frustration.
- Respond in a calm manner, reflecting back to the person that they have been heard and their situation is understood.
- Always stay respectful. Try to restore a sense of justice for the person.
- Explain what options are available and encourage them to try one of these. If a person refuses to calm down and continues to be offensive or aggressive, politely ask the person to leave the premises. If they refuse, discontinue discussions with them and advise them the police are being contacted, then immediately call police.

Aggressive people can be unpredictable, so encourage staff to be cautious at all times

BOMB THREATS

Instruct staff that if they receive a threat, they should:

- stay calm
- not panic or make return threats
- listen carefully for any identifying information from the caller, including a general description such as gender, age and any background noises
- ask the caller:
  - what the threat is
  - when the threat is to be carried out
  - where the threat may be located.
- keep the person talking for as long as possible (to obtain as much information as possible)
- once a call is finished DO NOT HANG UP - it may be possible to trace the call
- ensure all information has been written down
- inform management and report the threat to police immediately.

EVACUATION

- If evacuation is deemed necessary, it should be conducted in a pre-planned and organised manner.

LOCATING AN ITEM

If an item or suspect package is located:

- do not touch, tilt or tamper with the item
- notify police immediately and follow the instructions given to you by them
- clear all people from the area.

REPORTING A CRIME

EMERGENCIES

Call Triple Zero (000) when there is an emergency. For example any situation where life or injury is threatened, or any event that may cause danger to people or property.

NON-EMERGENCIES

Call 131 444 for non-urgent police assistance. For example reporting a crime that has already happened, reporting a missing person or making general police related enquiries.

Report information about criminals and their suspicious activities to Crime Stoppers on 1800 333 000 or at www.sa.crimestoppers.com.au. If you see something or hear something, say something. Rewards are available and you can remain anonymous.

Call Triple Zero (000) in an emergency or 131 444 for non-urgent police assistance

PROPERTY MARKING AND RECORDING

Police can trace your property if marked with your driver's licence number or Australian Business Number (ABN).

- All property should be clearly and permanently marked with the name of your business or your Australian Business Number (ABN). Your property could also be marked with your driver's licence number prefixed by the letter 'S' for South Australia, e.g. S123456, or business name and suburb.
- Record descriptions, models and serial numbers of your property and keep in a safe place on and offsite. Serial numbers are essential in identifying property.
- Include any identifying features such as dents, scratches or any individual marks of recognition.
- Property which cannot be marked should be photographed.

Serial numbers are essential in identifying property

SAPOL BUSINESS SECURITY ASSESSMENT

Please answer each question in this Business Security Assessment. If you answer 'No' to any question, refer to the **Suggested Treatments** in this booklet to improve your business security.

	YES	NO	COMMENTS
BUILDING IDENTIFICATION AND VISITOR ACCESS			
1 Is the business number clearly visible from the street?			
2 Is the business name clearly displayed?			
3 Are entry points to your business supervised?			
4 Are visitors allowed entry to your building by appointment only?			
5 Do they have to report to a reception area before entry?			
6 Are visitors asked for proof of identification?			
7 Are visitors asked to sign in when they enter the building?			
8 Are they provided with visitor passes?			
9 Are visitor passes designed to look different from staff identification?			
10 Are there appropriate signs identifying staff only areas?			
11 Are visitors allowed to take bags into the premises?			
12 Is a cloak/bag holding service provided at the point of entry?			
13 Does a member of staff accompany visitors at all times while in the building?			
14 Are there appropriate internal signs to guide visitors?			
15 Are visitor passes collected from visitors when they leave the building?			
16 Do staff wear identification badges at all times when in the building?			

	YES	NO	COMMENTS
17 Are reception/counter heights appropriate for your type of business?			
18 Are visitors/customers prevented from accessing the area behind the counter?			

FENCES AND GATES

	YES	NO	COMMENTS
19 Does the premises have perimeter fencing?			
20 Does fencing clearly delineate the premises boundary?			
21 Are the fences constructed at an appropriate height?			
22 Are gates in the perimeter fence able to be secured?			
23 Are the security measures on gates sufficient to prevent forced entry (e.g. by a vehicle)?			
24 Are there appropriate warning signs displayed around the perimeter of the premises?			
25 Are the fixings for the building coverings secured so that they cannot be released or removed from the outside?			

DOORS

	YES	NO	COMMENTS
26 Are door frames of solid construction?			
27 Are these doors fitted with quality locks to restrict access?			
28 Are there good quality locks on each accessible door above ground level?			
29 Are all locks in good working order?			
30 Can internal doors be locked when left unattended for long periods of time?			
31 Are security/screen doors installed?			

WINDOWS

	YES	NO	COMMENTS
32 Are windows of good construction?			
33 Are these windows fitted with quality locks to restrict access?			

	YES	NO	COMMENTS
34 Are unused windows permanently closed and secured?			
35 Are windows able to be locked in a partially open position?			
36 Are skylights suitably secured?			
37 Are windows free of promotional materials?			
38 Do you nominate staff to check that all doors and windows are closed and locked at the end of the business day?			

SECURITY LIGHTING

	YES	NO	COMMENTS
39 Is there security lighting installed around your premises?			
40 Does the security lighting work?			
41 Are entry and exit points adequately lit?			
42 Does the security light provide adequate coverage to light darkened areas?			

LANDSCAPING

	YES	NO	COMMENTS
43 Can people see your premises clearly from the street?			
44 Have all potential outdoor hiding spots been identified?			
45 Is landscaping well maintained to encourage good visibility around the perimeter of your premises, e.g. cutting back overgrown planting?			
46 Is graffiti promptly removed?			
47 Are bins secured in or away from buildings to stop them being used as a climbing aid and to discourage arson?			

SECURITY ALARM SYSTEMS

	YES	NO	COMMENTS
48 Is the premises protected by a security alarm system?			
49 Is the security alarm system monitored?			
50 Does the security alarm system have a duress facility?			

	YES	NO	COMMENTS
51 Does the system work?			
52 Is the security alarm system used?			
53 Are your staff familiar with the procedures for turning the system on and off?			
54 Is the system tested on a regular basis?			

CLOSED CIRCUIT TELEVISION (CCTV)

	YES	NO	COMMENTS
55 Do you have CCTV equipment installed?			
56 Are cameras monitored?			
57 Do the CCTV cameras cover the entrances and exits to your building?			
58 Do you have CCTV cameras covering critical areas in your business, such as server rooms or cash offices?			
59 Are CCTV images stored in accordance with the evidential needs of the police?			
60 Could you positively identify an individual from the recorded images on your CCTV system?			
61 Is your floor design arranged to provide good sightlines within the premises?			

SAFES

	YES	NO	COMMENTS
62 Do you have a safe installed?			
63 Is the safe securely anchored?			
64 Is the safe in an appropriate position?			
65 Does the safe have a drop-chute facility?			
66 Is the safe kept locked?			

CASH HANDLING

	YES	NO	COMMENTS
67 Do you have established cash-handling procedures?			
68 Do you have a lockable cash drawer?			
69 Do you have irregular banking procedures?			
70 Is a company used to transport cash?			
71 Is money counted out of public view?			

	YES	NO	COMMENTS

KEYS AND VALUABLES

	YES	NO	COMMENTS
72 Do you maintain a key register?			
73 Are all spare keys secured?			
74 Are keys to the safe adequately secured?			
75 Do staff have a location to secure their personal items?			
76 Does this location have restricted access?			

INFORMATION SECURITY

	YES	NO	COMMENTS
77 Do you lock away all business documents at the close of the business day?			
78 Do you have a clear-desk policy out of business hours?			
79 Do you close down all computers at the end of the business day?			
80 Are all your computers password protected?			
81 Are computer passwords changed regularly?			
82 Do you have computer firewall and antivirus software on your computers?			
83 Do you regularly update this protection?			

COMMUNICATION

	YES	NO	COMMENTS
84 Do you have a security policy showing how security procedures should operate within your business?			
85 Is this documentation regularly reviewed and if necessary updated?			
86 Do you have a senior manager who takes responsibility for security within your business?			
87 Do you regularly meet with staff and discuss security issues?			
88 Do you encourage staff to raise their concerns about security?			
89 Are you a member of a local Business Watch or a similarly constituted group?			

	YES	NO	COMMENTS
90 Do you speak with neighbouring businesses on issues of security and crime that might affect you all?			
91 Do you remind your staff to be vigilant when travelling to and from work, and to report anything suspicious to police?			

EMERGENCIES

	YES	NO	COMMENTS
92 Are your telephones pre-programmed with emergency contact numbers?			
93 Are your telephone lines tamper proof?			
94 Are staff trained to handle emergencies such as nuisance phone calls, bomb threats, fire safety, and workplace violence?			
95 Are staff trained to report maintenance problems and Occupational Health and Safety concerns?			

PROPERTY IDENTIFICATION

	YES	NO	COMMENTS
96 Have you recorded the make, model and serial numbers of your business items (such as mobile phones, computers etc)?			
98 Is all valuable property permanently marked with a corporate identifier (such as ABN)?			
98 Is your property photographed for easy identification?			
99 Do you have insurance?			
100 Are your property list and photographs adequately secured?			

SUGGESTED TREATMENTS

If you answered 'No' to any of the questions in the Business Security Assessment we suggest you consider making some changes. These changes will help reduce the risk to you, your business, your staff and customers.

BUILDING IDENTIFICATION AND VISITOR ACCESS
- The street and shop number must be displayed at the front of your business. This will assist emergency services and visitors to locate your property.
- Visitor access should be monitored and controlled at all entries into the building.
- Passes can assist in properly differentiating between visitors, maintenance and repair people and staff. These passes should be worn and be clearly identifiable at all times.
- If you are in any doubt, ring their company to check their authenticity.
- Effective signage and directions will provide guidance to visitors in locating reception areas and keep visitors away from restricted areas.
- Install height markers on the inside of your doors; this will help you judge the height of offenders in the event of crime.

FENCES AND GATES
- The boundary of the premises should be clearly defined by boundary fences, preferably an open-style construction. This allows greater visibility to and from the street, restricts unauthorised access and clearly defines your territorial space.
- Gates should be secured with quality hardened or alloy chains and padlocks.

- All gates should be kept shut and locked when not in use.
- Bollards or barriers can be installed to reduce the opportunity of vehicle assisted crime.
- Fences and gates should be regularly maintained to assist with the protection of your property.
- Warning signs should be strategically posted around the perimeter of your property, particularly near entry/exit points to warn intruders of security measures:
  - warning: these premises are under constant surveillance
  - warning: trespassers will be prosecuted
  - warning: no large amounts of money kept on premises
  - warning: monitored alarm in operation.

DOORS AND WINDOWS
- External doors and window frames should be of solid construction and comply with the Australian Standards and Fire Regulations (Australia Building Code).
- Doors should be fitted with quality deadlocks which comply with the Australian Standards and Fire Regulations (Australia Building Code).
- Windows should be fitted with key-operated window locks to restrict unauthorised access.
- Glass can also be reinforced to restrict unauthorised access by applying shatter-resistant film, replacing the existing glass with laminated glass or installing metal security grilles or shutters.
- No more than 15% of the display area of windows should be covered with promotional materials so that surveillance opportunities to and from the business are maximised.
- The roof should be reinforced with mesh below the roofing to restrict unauthorised entry.

SECURITY LIGHTING

- Install security lighting in and around your business, particularly over entry/exit points to create an even distribution of light with no glare, e.g. sensor lighting, floodlighting.
- Consider installing sensor lighting which is cost effective as it only activates when movement is detected within the zone.
- Leave a limited amount of internal lighting on at night to enable patrolling police, security guards or passing people to monitor activities within the business.
- The power board should be housed within a cupboard or metal cabinet and secured with an approved electricity authority lock to restrict unauthorised tampering with the power supply.

LANDSCAPING

- Landscaping should be maintained regularly with trees and shrubs trimmed away from doors and windows.
- Keeping trees and shrubs trimmed can reduce concealment opportunities and increase visibility when travelling to and from the business.
- Remove obstacles and rubbish from property boundaries, footpaths, driveways, car parks and buildings to restrict concealment and prevent offenders scaling your building.

SECURITY ALARM SYSTEMS

- To enhance the security of your business, you can install a monitored intruder alarm system.
- If you have a system installed within your business, make sure you use it.
- Ensure the system has been designed and installed to the Australian Standards.

- Consider incorporating a duress facility into the system to enable staff to activate the system manually in the event of an emergency, such as a robbery.
- LEDs (Light Emitting Diodes) are red lights within the detectors. They should be deactivated so that offenders cannot test the range of the system.
- The system should be tested on a regular basis to ensure that it is operating effectively.
- Staff should be trained in the correct use of the system to reduce the activation of false alarms.
- Alarm system controls should be concealed to restrict tampering.
- Remote on/off switches should be strategically located.
- Movement detection devices should be strategically located around the premises.

CLOSED CIRCUIT TELEVISION (CCTV)

- CCTV can enhance the physical security of your business and assist in the identification of people involved in anti-social or criminal behaviour.
- Cameras should be installed both within and around the business to maximise surveillance opportunities.
- Digital or video technology should be used to record images from the cameras.
- Cameras should monitor the cashier's area, high cost merchandise or areas with poor natural supervision.
- TV monitors should enable staff to monitor activities on the camera.
- Recording equipment should be installed away from the counter area to avoid tampering.
- Videotapes need to be replaced regularly to maintain quality images.
- If a surveillance system is installed, use it.

- Staff should be trained in the correct use of the system.
- Any surveillance system should be manufactured and installed by a qualified and reputable company and regularly function tested.

SAFES

- A safe designed and installed to the Australian Standards can provide additional security for money and other valuables.
- Anchor the safe to the floor to prevent easy removal and install it in an area where access is limited and away from public view.
- The safe should have a drop-chute facility so that staff can deposit money without having to open it.
- Consider a time delay lock, which means that the safe can only be opened at a particular time (or times) each day.
- The safe should be locked at all times when not in use to restrict access.

CASH-HANDLING

- Establish clear cash-handling procedures within your business to reduce opportunities for crime.
- Try to reduce the amount of cash your business deals with.
- Limit the amount of money carried in the cash drawer at any time. Use as small a float as is practical for your business.
- Lock cash drawers when not in use and clear money from the cash drawer on a regular basis, e.g. to a safe.
- If possible, have a secure area for handling and counting cash. ALWAYS keep this area secure and out of sight of the general public and access ways.

- Use a minimum of two staff, or security services, when personally transferring money to or from the bank.
- Consider using a reputable security company to do your banking especially when transferring large amounts of money.
- Where possible, limit cash amounts by installing electronic payment systems such as EFTPOS.
- Don't use conspicuous bank-bags when transferring money.
- Avoid wearing uniform or identification when moving money to or from the bank.

KEYS AND VALUABLES CONTROL

- The control of keys and valuables should be closely monitored by management.
- A key register should be used to list those staff members who have been issued with keys, the type of keys issued and the areas each staff member has access to.
- Registers should be detailed and regularly maintained and audited.
- To reduce the likelihood of theft and or damage, try to limit the number of keys and valuables left unsecured or in plain sight of potential intruders.

INFORMATION SECURITY

- Limit access to confidential information.
- Sensitive material and confidential records should be shredded when no longer required.
- Computer passwords should be changed regularly to restrict access and avoid misuse by past and present staff.
- Cancel access promptly when people transfer or leave.

COMMUNICATION
- Staff training days should be held on a regular basis reinforcing safety and security procedures of your business.
- Emergency evacuation plans should be implemented, maintained and prominently displayed.
- Have clear policies on critical issues such as shoplifters, handling aggressive customers and cash handling.
- Encourage employees to report any suspicious activity or persons in or around the area to local police.

EMERGENCIES
- Telephones should be pre-programmed with the emergency number '000' and your local police number for quick reference.
- Telephone lines or boxes should be secured with an approved lock to avoid unlawful tampering.
- Make sure staff are familiar with emergency procedures and what they can do if they feel unsafe in the workplace.
- Keep a copy of a Bomb Threat Checklist under all telephones and ensure staff understand the form's purpose and how to fill it out.
- Report threats to the police immediately.
- Suspicious items - what to look out for:
  - excessive or stained wrapping
  - no return address or markings such as 'Confidential, Private'
  - incorrect titles or misspelling of common words
  - excessive postage or weight
  - unexpected or unsolicited mail.

- Do not touch, tilt or tamper with the item. Contact police immediately on '000'. Explain what it is that makes the package suspicious. Follow the instructions given to you by police.

PROPERTY IDENTIFICATION
- Record descriptions, model information and serial numbers of all business property for easy identification.
- Engrave your property with a traceable number such as your ABN (Australian Business Number) for identification.
- For items that cannot be engraved, you may wish to mark them with an ultra-violet pen. This marking is only visible under an ultra-violet (black) light.
- When you sell your property, place a neat line through your engraving to show that it is no longer valid. It is also a good idea to give the person a receipt to prove the sale of the item.
- Photograph and record the details of unique items to aid in their recovery if stolen.
- Your property list, photographs and other documentation should be adequately secured, e.g. in a safe or safety deposit box.

CONCLUSION

By completing this assessment and implementing suggested treatments you are helping to reduce the opportunity of crime. SAPOL encourages you to obtain you own independent advice as to the safety and security of your business. Should you require further information on the subjects listed in this assessment, please contact your nearest police station.

SAPOL would like to thank you for your interest in improving the security of your business and in preventing crime in our community.

STICKER INSTRUCTIONS

- Place the 'No cash' sticker in a prominent position at the entry point of the premises.
- Place the 'Height' sticker either near the entry or near the counter area. Use a tape measure to ensure all heights are accurate.
- Place the 'Keep cash low' sticker near your cash transaction area.

The security assessment and suggested treatments have been reproduced with the permission of the NSW Police.

For further crime prevention assistance, please contact your local
SAPOL Crime Prevention Section or visit www.police.gov.au

Become a local Business Watch member. For further details visit www.watchsa.com.au