It is our responsibility to protect our information and our assets wisely.

Assess your own situation and make sure you are playing your part in protecting yourself and your organisation.

Find out more

Personnel security requirements are detailed in the South Australian Government Protective Security Management Framework.

Ensure you report potential insider threats or suspicious activity to your Agency Security Executive.
Organisations are spending increasing amounts of time and money protecting employees, systems and information from external threats.

While this is important, there is greater opportunity for a person inside the organisation to abuse or facilitate access to information and assets that could put your organisation at risk.

Insider threat is one of the most significant risks facing organisations. As insiders are trusted colleagues, they can be harder to identify.

All government employees have a responsibility to protect government information, and to understand how to spot an insider threat.

The security of an organisation relies on the integrity of its people - security is everyone’s job.

Who is an insider?

An insider is a person who has or had trusted access to an organisation’s information, resources and systems. This can include current and former employees, contractors, business partners and vendors who are in a position to exploit these resources.

What is an insider threat?

Insider threat includes activities that actively or passively put an organisation and its assets at risk. This can happen through unauthorised information sharing, misclassification of information, sabotage or malicious damage, corruption, theft of assets or intellectual property, or enabling access to outsiders.

Insider threat is categorised in two ways - intentional and unintentional.

Intentional threats exist where there is deliberate intent to harm the organisation. It can be motivated by:
• criminal financial gain
• disgruntlement
• revenge
• thrill-seeking
• terrorist/ideological/espionage purposes - either personal, corporate or state-sponsored.

Unintentional threats exist where an insider is deceived into harming the organisation, or does not understand the value of the information they hold. Examples include:
• Social engineering - an individual is deceived into providing information relating to personnel, ICT systems, or security processes.
• Phishing scams - attempts to obtain confidential information or access to systems, typically in the form of an email that appears to be from a legitimate and trusted source.

Regardless of the motivation, insider threat can cause damage to your organisation. Fixing this damage can be expensive, time consuming, detrimental to reputation and disruptive to operations.

What to look for

You can help to reduce insider threat by being aware of unusual behaviour. It could be:
• An employee working odd hours without genuine need to do so.
• People asking questions about classified/sensitive information.
• Unauthorised personnel gaining access to buildings, information, ICT systems or people.
• Significant, unexplained change in the personal or financial circumstances of a fellow employee.
• Colleagues experiencing considerable stress, anxiety, or decrease in work performance.

What you can do

Across your organisation:
• Assess your data, employees and assets, and prioritise the risks associated with them.
• Ensure your risk management framework includes a fraud and corruption control policy and a security risk management policy.
• Refer to your Agency Security Plan. Your plan should consider ways to prevent, detect and respond to an insider threat.

Management of staff and contractors:
• Pre-employment security, identity and criminal checks help build a good security culture.
• Classify job roles correctly and apply personnel screening as needed. Regularly analyse and update job descriptions to reflect positions of trust.
• Encourage employees to report threats as a normal part of your operations.
• Implement Information Security Awareness Training to demonstrate to employees the value of their information.
• Exiting is as important as inducting. When an employee leaves, ensure all ICT and physical access is terminated according to policy.
Introduction

Organisations are spending increasing amounts of time and money protecting employees, systems and information from external threats.

While this is important, there is greater opportunity for a person inside the organisation to abuse or facilitate access to information and assets that could put your organisation at risk.

Insider threat is one of the most significant risks facing organisations. As insiders are trusted colleagues, they can be harder to identify.

All government employees have a responsibility to protect government information, and to understand how to spot an insider threat.

The security of an organisation relies on the integrity of its people - security is everyone’s job.

Who is an insider?

An insider is a person who has or had trusted access to an organisation’s information, resources and systems. This can include current and former employees, contractors, business partners and vendors who are in a position to exploit these resources.

What is an insider threat?

Insider threat includes activities that actively or passively put an organisation and its assets at risk. This can happen through unauthorised information sharing, misclassification of information, sabotage or malicious damage, corruption, theft of assets or intellectual property, or enabling access to outsiders.

Insider threat is categorised in two ways - intentional and unintentional.

Intentional threats exist where there is deliberate intent to harm the organisation. It can be motivated by:

• criminal financial gain
• disgruntlement
• revenge
• thrill-seeking
• terrorist/ideological/espionage purposes - either personal, corporate or state-sponsored.

Unintentional threats exist where an insider is deceived into harming the organisation, or does not understand the value of the information they hold. Examples include:

• Social engineering - an individual is deceived into providing information relating to personnel, ICT systems, or security processes.
• Phishing scams - attempts to obtain confidential information or access to systems, typically in the form of an email that appears to be from a legitimate and trusted source.

Regardless of the motivation, insider threat can cause damage to your organisation. Fixing this damage can be expensive, time consuming, detrimental to reputation and disruptive to operations.

What to look for

You can help to reduce insider threat by being aware of unusual behaviour. It could be:

• An employee working odd hours without genuine need to do so.
• People asking questions about classified/sensitive information.
• Unauthorised personnel gaining access to buildings, information, IT systems or people.
• Significant, unexplained change in the personal or financial circumstances of a fellow employee.
• Colleagues experiencing considerable stress, anxiety, or decrease in work performance.

What you can do

Across your organisation:

• Assess your data, employees and assets, and prioritise the risks associated with them.
• Ensure your risk management framework includes a fraud and corruption control policy and a security risk management policy.
• Refer to your Agency Security Plan. Your plan should consider ways to prevent, detect and respond to an insider threat.

Management of staff and contractors:

• Pre-employment security, identity and criminal checks help build a good security culture.
• Classify job roles correctly and apply personnel screening as needed. Regularly analyse and update job descriptions to reflect positions of trust.
• Encourage employees to report threats as a normal part of your operations.
• Implement Information Security Awareness Training to demonstrate to employees the value of their information.
• Exiting is as important as inducting. When an employee leaves, ensure all ICT and physical access is terminated according to policy.
Insider Threat
- A guide for managers

It is our responsibility to protect our information and our assets wisely.

Assess your own situation and make sure you are playing your part in protecting yourself and your organisation.

Find out more

Personnel security requirements are detailed in the South Australian Government Protective Security Management Framework.

Ensure you report potential insider threats or suspicious activity to your Agency Security Executive.