Australian Government

Australian Security Intelligence Organisation

T4 Protective Security

# Security managers guide

## Working from home

www.asio.gov.au

Release history

| Issue no. | Issue date | Description |
|---|---|---|
| 1.0 | March 2020 | First release |

Handling instructions

This document is UNCLASSIFIED.

Disclaimer

The information provided in this document is intended to be used as general guidance material only and is not provided for any other purpose. In particular it is not intended to provide comprehensive advice on its subject matter or in relation to any particular product, and should not be relied on as providing such advice. Organisations or individuals using or relying on the information contained in this document are deemed to do so in conjunction with their own judgement and assessment of the information in light of their particular needs and circumstances. The Australian Security Intelligence Organisation (ASIO) has taken every care in the preparation of this document to ensure that the information is accurate at the time of publication. The Commonwealth, its officers, employees and agents exclude all liability for loss or damage (including in negligence) suffered or incurred by any precinct or individual as a result of their use of or reliance on the information contained in this document.



FOI statement

This document, and any information, extract or summary from this document, is exempt under the *Freedom of Information Act 1982*.

## Contents

## Introduction

This guide provides advice on protective security practices that can be implemented where usual security practices are either suspended or changed due to increased numbers of staff working from home. These arrangements will not be new to many organisations and staff, but current events are forcing organisations to consider home working on a greater scale, and for unexpectedly longer periods of time.

The threats—from hostile foreign intelligence services through to low–level criminals—will not be reduced by current events. Threat actors will adapt to take advantage of a distracted organisation. It is important that staff are aware of the threats and risks of working from home, and take appropriate steps to adapt to difficult and new circumstances.

Further information is available in the Australian Security Intelligence Organisation's (ASIO) analytical report, AAR 025/2020 of 25 March 2020, *Australia: security implications of COVID–19*.

Organisations can subscribe to ASIO's Outreach website to access AAR 025/2020 of 25 March 2020 and the complete suite of ASIO–T4 security manager guides.

## Purpose

This guide assists security managers to prepare their organisation for an increase in home–based work and identify security measures that can be implemented for the protection of information, people and assets in the changing work environment.

Security managers should note that, even with the implementation of security measures detailed in this guide, the design and construction of most private residences only provides a basic level of security, and would not protect against a determined and skilled adversary.

The advice in this guide is not exhaustive and is non–mandatory.

## Risk assessment

Organisations should conduct a risk assessment to identify and consider likely threat (intent and capability) and risk (likelihood and consequence) scenarios to inform their assessment of additional security measures required at a home residence. The activities being undertaken and the information being stored, handled, processed and discussed at a home residence will change the assessment of the risk of information being compromised.

Organisations will be vulnerable to different types of threats—the risk level of these threats will depend on an organisation's services, intellectual property, data holdings, public profile, size and location. However, it is important to note that foreign intelligence services, foreign officials, and politically, commercially or issue–motivated groups and individuals can devote considerable effort and resources to gaining access to political, economic, scientific, technological, military and other information. This can include privileged and personal information that is not available to the general public.

Organisations should consider whether the following is relevant as part of the risk assessment process:

- Are occupants or personal property inside the residence a desirable or high–value target?
- Have changes to the security environment exposed occupants to new security threats or increased risk?
- Is there a credible threat to the organisation and/or the occupants?
- Does the local area have a high or increasing crime rate[1]?
- Is the crime rate high compared with other local regions or cities?
- Are there industrial, commercial or government facilities located in the local area which are prone to criminal activity?
- Are there physical signs of antisocial behaviour in the local area, such as graffiti and vandalism?
- Are there recurring complaints or concerns from local residents about security, or fear of crime.

Home–based work increases the risk of compromise of sensitive information, which can cause damage to an organisation's reputation.

1 Crime statistics are available from different organisations in each state and territory, such as police, Neighbourhood Watch, local government and crime statistic agencies

## Home residence security assessment

Staff should be encouraged to conduct a self–assessment of their home residence to assess whether existing security measures are adequate to protect the organisations assets, or whether further treatments are needed to reduce risks to the organisation's acceptable level.

The security measures implemented for home–based work should restrict access to sensitive information and use the most secure communications available.

Organisations should refer to ASIO's T4 Protective Security (ASIO–T4) security managers guide *Private residence physical security assessment* for advice on protecting people and physical assets from low–level criminal risks—this guide is available on ASIO's Outreach website, www.outreach.asio.gov.au.

## Policy and procedures

The organisation's working from home security policies and procedures should provide assurance that sensitive organisation information and assets are protected in accordance with the organisation's level of risk tolerance.

An organisation's policy and procedures should include clear guidance on:

- What is allowed: printing, cameras, microphones, use of social media, bring–your–own–device, connecting to wi–fi networks and accessing websites?
- What is not allowed; for example, financial transactions, processing of sensitive or personal data, or some information technology (IT) roles?
- What is required for the transport and destruction of sensitive material and assets, including mobile devices and removable media?
- Whether maximum storage periods apply for certain information or assets in a residential setting?
- The organisation should consider:
- a formal employee briefing and agreement that the employee understands and will comply with all procedures and security requirements;
- the organisations security, workplace health and safety, and human resources policies and procedures apply when working from home should be followed;
- any financial expenses, taxation and insurance obligations incurred, either by the organisation and/or the staff member;
- a regime for ongoing, regular compliance audits; and
- a process for employees to return information and assets to secure facilities, once the need for extended working from home arrangement has passed.

Any changes to working from home security policies and procedures should be communicated clearly to the whole workforce. Consideration should be given to the length of time the arrangements will be in place. Periodic inspections and audits of higher–risk staff, residences and assets should be undertaken if arrangements continue for an extended period of time.

### Security awareness

Working from home reduces the contact time between security and staff; therefore, regular, varied and consistent security awareness becomes even more important. Organisations should ensure that the workforce is given appropriate security awareness training, especially for those inexperienced at working remotely and using new technology.

This could include:

- identifying continued security threats and risks;
- maintaining the need–to–know principle;
- being vigilant and reporting any suspicious activity or incidents; and
- continuously seeking to identify and suggest improvements to security.

Clear instructions should be provided to staff on how to report security incidents, and any action to be taken. For example:

- A staff member unwittingly clicking on a phishing email. Staff should be educated to notify the IT department, change compromised passwords and follow instruction from the security teams.
- A mobile device or removable media is lost or stolen. Staff should notify the IT department so that remote mobile device management can be used to limit the compromise of information, their line manager so that actions can be taken to limit the impact of compromised information and the police to commence an investigation.

Encourage staff (in a positive, blame–free manner) to report any loss or potential loss as soon as possible. Early reporting may minimise the extent of information loss, and staff who fear reprisals are less likely to report promptly.

## Mobile device security

Mobile devices can allow staff to remotely access their organisation's sensitive networks, information or capabilities. There are several mitigations that an organisation can implement to reduce security risks associated with mobile devices and working from home.

- Ensure that the organisation systems and applications, including virtual private networks, firewalls and remote desktop clients are up–to–date with the most recent security patches installed.
- Implement multi–factor authentication for remote access systems and resources (including cloud services).
- Virtual Private Networks (VPNs) allow remote users to securely access an organisation's IT resources, such as email and file services. VPNs create an encrypted network connection that authenticates the user and/or device, and encrypts data in transit between the user and the organisation's data. If your organisation is already using a VPN, make sure it is fully patched. Additional licenses, capacity or bandwidth may be required to support increased working from home arrangements.
- Ensure that staff are informed and educated in cyber security practices, such as detecting socially engineered messages and not clicking on suspicious links or files.
- Devices used for working outside an office environment are more vulnerable to theft and loss. Whether they are using their own device or the organisation's, ensure staff understand the risks of leaving them unattended, especially in public places. When the device is not being used, encourage staff to keep it somewhere safe. Make sure devices encrypt data whilst at rest, which will protect data on the device if it is lost or stolen. Most modern devices have encryption built in, but encryption may still need to be turned on and configured.
- Ensure staff understand the importance of keeping software (and devices) up to date, with regular reminders.
- The majority of devices include tools that can be used to remotely lock access to the device, erase stored data, or retrieve back–up data. Organisations should use mobile device management software to set up devices with a standard protection configuration.
- Make sure staff know how to report any mobile device problems. This is especially important in a security context, where this may indicate compromise to a device.

- USB drives can contain large amounts of sensitive information and can be easily misplaced. These devices are also an easy way to introduce and share malware throughout information and communications technology systems. When USB drives and cards are openly shared, it becomes hard to track what they contain, where they have been and who has used them. You can reduce the likelihood of infection by:
  - disabling removable media using mobile device management settings;
  - using antivirus tools where appropriate;
  - only allowing products supplied by the organisation to be used;
  - protecting data at rest (encrypt) on removable media; and
  - requesting that staff transfer files using alternative means (such as corporate storage or collaboration tools), rather than via USB.
- Organisations should establish records for sensitive information, assets and mobile devices which are removed from their sites, particularly if held for significant periods of time by staff working from home. These should be checked–in when staff return to work.
- The protection of mobile devices, and the information that they can store and access, is enhanced by the situational awareness of the user and their ability to minimise risks when conducting work outside the office. Oversight and overhearing risks can be mitigated by selecting appropriate locations to use devices.

Further information can be found at www.cyber.gov.au.

### Personal and personnel security

Organisations should provide ongoing support and guidance to the workforce, especially those who are working from home; covering technical, security, and wellbeing issues. This will improve workforce morale and minimise risks to the organisation from malicious insider threats. This could include:

- using ongoing, varied and regular security awareness updates, reminding staff of the continued security threat;
- conducting virtual personnel security briefings for new staff, separating staff and those undertaking new roles;
- conducting virtual interviews for employment screening, ongoing human–resource (HR) matters or security investigations;
- encouraging line managers to regularly contact staff through team and one–on–one contact methods. This assists business objectives and improves staff wellbeing;

- line managers should be aware of changes in personal circumstances that put additional stress on their employees, such as financial concerns and ill–health. Concerns should be reported and managed in collaboration with the line manager, security and the organisation's HR area;
- the organisation should ensure that the workforce has remote access to work health and safety and employee counselling services, if required, during periods of high anxiety;
- frequent reminders to the workforce of the importance of reporting security concerns, even when working remotely, and how to do so;
- assisting staff to manage their digital footprint; such as, managing privacy settings on social media, protecting personal information and limiting discussion of working–from home arrangements and locations, especially on social media; and
- long–term working from home can erode an organisation's shared security culture. Organisations should monitor security culture as much as they can, and provide ongoing education and awareness to staff on their security responsibilities.

### Physical security

The physical security of a private residence is important to protect the organisation's sensitive information and the personal security of the organisation's employees. Organisations should ensure that staff working from home have physical security measures in place. This minimises the risk that an organisation's assets and information may be accessed, used, modified, or removed from the premises without authorisation.

There are a number of physical security measures, including associated actions by owners, that can be used to improve the security of private residences. An additional benefit to the employee is that these physical security improvements and procedures can help protect them from low–level criminal risks.

When providing advice on residential security measures, security managers should adopt a risk management approach, taking into consideration the threat environment and local crime statistics. The physical security requirements of employees' residences depends on an employee's position, profile, access and location.

In general, the following measures will help improve the security of physical private residences.

- The exterior—use adequate lighting and a well–designed landscape and garden to allow natural surveillance
- The perimeter—using barriers and security hardware to remove the opportunity of easy access, such as locks and alarm systems. Some systems can be used safely and effectively even when the residence is occupied.

Staff may live in shared accommodation with people not employed by the organisation. Specific security risks around working from home can include oversight and overhearing by unauthorised people. Simply closing a residence door, or closing blinds and curtains, can mitigate the risk of oversight, but this is unlikely to reduce normal speech to an unintelligible level. Staff should be aware of their surroundings, and who may be accidentally or deliberately listening to their conversations. Organisations should provide security advice on:

- what may or may not be discussed with house–mates or family members;
- the use of sensitive information in the company of house–mates or family members; and
- the use of an organisation's devices by housemates or family members.

It is recommended that sensitive information, removable media and mobile devices are stored in a lockable container. Ideally a designated, lockable room should be used for sensitive home–based work.

Sensitive information, removable media and mobile devices should be sanitised or destroyed before disposal. Hard copy information should be cross–cut shredded before disposal. Sanitisation and destruction could take place at the residence, or on return to the organisation's secure facilities.

Further information can be found in ASIO–T4 *Security managers guide: Private residence security*. Organisations can subscribe to ASIO's Outreach website to access the complete suite of ASIO–T4 security manager guides.

### Existing facilities

If the majority of an organisation's staff are working from home, there may be reduced staffing at offices and facilities, which will require adjustments to security policies and procedures.

Individuals that remain in offices or facilities may take advantage of relaxed security procedures or minimal supervision for unauthorised purposes. It is vital that organisations are aware of how existing security measures at the site have changed and what provisions have been made to minimise any vulnerabilities.

Consideration should be given to:

- ensuring an organisation's guard force are aware of any changes to security policy regarding entry and exit, removal of sensitive material from the site and increasing vigilance to those breaching the rules either by accident or deliberately.
- if fewer members of the workforce are present, to observe and enforce good security behaviours and having a greater reliance upon technical measures to prevent deliberate or accidental security breaches.
- frequent reminders to staff on both the physical and technical security measures that should be adopted. These should include guidance on when and how to report security concerns.
- recognising signs of disgruntlement from within the workforce, specifically where staff are being put on temporary absence, receiving reduced pay or conversely from those required to continue working whilst covering for absent staff.
- Auditing open–source information and increasing deterrence communications during periods of heightened vulnerability. Further information can be found in ASIO–T4 *Security managers guide: Deterrence Communications*.

## Conclusion

There are a number of organisational and personal security threats when working from home. The risks and vulnerabilities to an organisation's information and personnel are not the same as when working in a dedicated fixed facility—the environment is less controlled and changes more frequently. The organisation must ensure their risk assessment is pragmatic and be aware that protective security objectives may have to be achieved within varied and less controlled environments.

## References and further reading


- United Kingdom Centre for the Protection of National Infrastructure, *Pandemic security behaviours*, March 2020
- United Kingdom Centre for the Protection of National Infrastructure, *Personnel security in remote working: a good practice guide*, February 2012
- United Kingdom National Cyber Security Centre, *Home working: preparing your organisation and staff*, 17 March 2020
- Australian Cyber Security Centre, *Cyber security is essential when preparing for COVID–19*, March 2020
- Australian Security Intelligence Organisation, *Security managers guide: Private residence security*, 2017
- National Threat Assessment Centre analytical report, AAR025/2020, *Australia: security implications of COVID–19*.



20-11656