Physical security management guidelines

Working away from the office

Approved
13 December 2011

Version 1.0
© Commonwealth of Australia 2011

All material presented in this publication is provided under a Creative Commons Attribution 3.0 Australia (http://creativecommons.org/licenses/by/3.0/au/deed.en ) licence.

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the CC BY 3.0 AU licence (http://creativecommons.org/licenses/by/3.0/legalcode).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the It's an Honour (http://www.itsanhonour.gov.au/coat-arms/index.cfm) website.

Contact us

Inquiries regarding the licence and any use of this document are welcome at:

Business Law Branch
Attorney-General’s Department
3-5 National Cct
BARTON ACT 2600

Telephone: (02) 6141 6666
copyright@ag.gov.au

<table>
<thead>
<tr>
<th>Document details</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Security classification</td>
<td>Unclassified</td>
</tr>
<tr>
<td>Dissemination limiting marking</td>
<td>Publicly available</td>
</tr>
<tr>
<td>Date of security classification review</td>
<td>December 2013</td>
</tr>
<tr>
<td>Authority</td>
<td>Protective Security Policy Committee</td>
</tr>
<tr>
<td>Author</td>
<td>Protective Security Policy Section</td>
</tr>
<tr>
<td></td>
<td>Attorney-General’s Department</td>
</tr>
<tr>
<td>Document status</td>
<td>Approved 13 December 2011</td>
</tr>
</tbody>
</table>
Contents

1. Introduction ........................................................................................................................................ 1
   1.1 Purpose ........................................................................................................................................ 1
   1.2 Audience ...................................................................................................................................... 1
   1.3 Scope .......................................................................................................................................... 1
       1.3.1 Use of specific terms in these guidelines .............................................................................. 1
       1.3.2 Additional terms used in these guidelines ........................................................................... 2

2. Background ........................................................................................................................................ 3
   2.1 Why the guidelines were developed ............................................................................................ 3
   2.2 Relationship to other documents .................................................................................................. 3
   2.3 How are these guidelines structured? ............................................................................................ 3

3. Working away from the office ............................................................................................................ 4
   3.1 Mobile computing and communications ........................................................................................ 4
   3.2 Tele-working .................................................................................................................................. 5
       3.2.1 Tele-working from home ........................................................................................................ 6
       3.2.2 Tele-working communications arrangements ........................................................................ 6
   3.3 Working away from the office without ICT support ...................................................................... 6

4. Personal safety when working out of the office .................................................................................. 7

5. Protecting agency information and physical assets ............................................................................ 8
   5.1 ICT security ................................................................................................................................... 8
       5.1.1 Use of an employee’s personal ICT equipment ..................................................................... 8
       5.1.2 Use of public ICT equipment, wireless networks and communications ................................ 9
   5.2 Physical protection of official information when away from the office ........................................... 9
       5.2.1 Classified information ........................................................................................................... 9
       5.2.2 Business information ........................................................................................................... 10
       5.2.3 Conversation security .......................................................................................................... 10
       5.2.4 Physical security of official information in private client facilities ...................................... 10
       5.2.5 Options for transferring information to remote locations ...................................................... 11
       5.2.6 Disposal of official information ............................................................................................ 11
   5.3 Protecting agency assets ............................................................................................................... 11
       5.3.1 Portable assets ....................................................................................................................... 12
       5.3.2 Security alarm system options ............................................................................................... 12
       5.3.3 Locating assets in private client facilities .............................................................................. 12
   5.4 Reporting incidents ....................................................................................................................... 13

6. Annex A—Checklist for mobile computing and communications/tele-working ....................... 14
7. Annex B—Useful Links ........................................................................................................ 16
   7.1 Telework agreements .................................................................................................. 16
   7.2 Personal safety ........................................................................................................... 16
   7.3 ICT security standards ............................................................................................... 16
## Amendments

<table>
<thead>
<tr>
<th>No.</th>
<th>Location</th>
<th>Amendment</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. Introduction

1.1 Purpose

The *Australian Government physical security management guidelines—Working away from the office* provides guidance to achieve a consistent approach to determining information and physical security controls when employees are working away from their agency's offices.

These guidelines assist agencies to protect their people, information and physical assets in situations where the people, information and assets are outside the immediate control of the agency.

1.2 Audience

This document is primarily intended for:

- Australian Government security management staff, and
- any other body or person responsible for the security of Australian Government people, information or physical assets outside of agency premises.

1.3 Scope

These guidelines relate to information and physical security measures employed by Australian Government agencies to identify and mitigate the security risks to official information and assets, and protect their employees, when working outside agency facilities.

These guidelines do not address security risks to employees who are working overseas. Agencies should contact the Department of Foreign Affairs and Trade for advice on security in overseas locations. General overseas travel advice is available from www.smarttraveller.gov.au.

Agencies with employees travelling overseas may also refer to the Defence Signals Directorate (DSD) publication *Travelling overseas with a laptop*.

Where legislative requirements prescribe higher controls than those identified in these guidelines then the controls required by legislation take precedence and need to be applied.

Agencies are to protect any information or physical assets provided by another government in accordance with international agreements; see PSPF Governance Arrangements – International security agreements.

1.3.1 Use of specific terms in these guidelines

In these guidelines the use of the terms:

- ‘need to’ refers to a legislative requirement that agencies must meet
- ‘are required to’ or ‘is required to’ refers to a control:
  - to which agencies cannot give a policy exception, or
  - used in other protective security documents that set controls.
- ‘are to’ or ‘is to’ are directions required to support compliance with the mandatory requirements of the physical security core policy, and
• ‘should’ refers to better practice; agencies are expected to apply better practice unless there is a reason based on their risk assessment to apply alternative controls.

For details on policy exceptions see the *PSPF - Australian Government Physical Security Management Protocol* (section 1.4).

1.3.2 Additional terms used in these guidelines

**Business impact levels**— see the *PSPF - Australian Government protective security governance guidelines—Business impact levels*.

**Business information**—that is unclassified information relating to agency business, including information bearing dissemination limiting markers.

**Mobile computing and communications**—Work from a non-fixed location using portable computing/communications devices—for example; laptops, notebooks, tablets, smart mobile phones and PDAs.

**Mobile employees**—Includes employees who work at multiple locations using their laptop, or other mobile computing device, as their primary ICT device—setting it up in hotels, offices, at home or in the field—for example, client support workers, who deal with clients outside the regular office environment.

**Private client facilities**—Facilities belonging to private industry clients which can be used by agency personnel to undertake agency work.

**Regional location**—Refers to any location away from an agency’s central office or major operational centres.

**Tele-centre**—A location separate to the employee’s home and remote from the agency’s normal business premises that provides access to an office environment and may provide remote access to agency ICT systems. These facilities may be provided on an agency specific or shared basis.

**Tele-work (telework, telecommuting)**—Paid work conducted away from an agency’s offices in a fixed location, which requires at least periodic connection to the employer’s ICT network. Tele-work is distinguished from mobile computing by having a controlled environment and little need for portability of equipment. Tele-work is subject to a formal agreement between the agency and the employee.

**Tele-workers**—An employee that undertakes tele-work, including:

- **Casual tele-workers**—Casual tele-workers take advantage of tele-working to meet a short-term or intermittent requirement. Unless there is a formal tele-work agreement then they should be considered mobile employees.

- **Full-time tele-workers**—Full-time tele-workers operate primarily from a remote, fixed location. This could be either the tele-worker’s own home or a remote office/tele-centre.

- **Part-time tele-workers**—Part-time tele-workers may spend part of their time working in a fixed remote location and part of their time in the office.

- **Day extenders**—Day extenders may work a regular day in the office and then may log in from a fixed remote location, normally from home, to continue to work or meet a short-term or intermittent requirement.

---

1 Full-time and Part-time in this context does not relate to a person’s employment status.
2. **Background**

2.1 **Why the guidelines were developed**

The Australian Government physical security management guidelines—Working away from the office have been developed assist agencies to manage the risks to, and to provide a consistent and structured approach to determining the security requirements for, employees working away from the office. These guidelines will:

- assist in establishing consistent terminology relating to working away from the office across the Australian Government, and
- give agencies a framework for the assurance needed to ensure the safety of agency personnel, information and assets.

2.2 **Relationship to other documents**

These guidelines support the implementation of the Protective Security Policy Framework (PSPF). In particular, they support the PSPF - Australian Government physical security management protocol and Australian Government information security management protocol, and associated guidelines.

Agencies are to implement ICT arrangements to meet:

- the Australian Government information security manual, and
- unless otherwise specified.

These guidelines should be read in conjunction with:

- Inter-Agency Security Forum (IASF) Unclassified Security Awareness Bulletin No. 03/07—Laptop Computer Security, and
- IASF Security Awareness Bulletin No. 02/07 - Personal electronic device security (FOUO)

The IASF guides are only available to agency security advisers (ASAs). They can be found at the Protective Security Policy Community of GovDex.

These guidelines were developed with regard to:

- *[Tele-working policy for ICT staff](#)* approved by the Secretaries ICT Governance Board on 17 December 2009, and

2.3 **How are these guidelines structured?**

These guidelines are divided into:

- working away from the office general requirements
- personal safety measures
- information and physical asset control measures, and
- a checklist for agencies reviewing working away from the office security measures.
3. Working away from the office

Working away from the office includes all work undertaken by the agency using mobile employees and tele-workers—that is they work outside of normal agency facilities.

The types of working away from the office that normally requires ICT support are:

- mobile computing and communications, or
- tele-working.

Mobile employees may undertake work away from the office without ICT support—for example using hard copy information. With the availability of mobile phones, personal computing devices and wireless computing, the instances of working away from the office where ICT support is not available, or required, are diminishing.

Working away from the office may include field work undertaken on behalf of the agency by contractors, but does not include any work undertaken by contractors in their own facilities. Agencies are to address any security requirements in these situations by specific terms and conditions in the contract. See PSPF Governance arrangements – Contracting.

3.1 Mobile computing and communications

Mobile computing and communications is work from a non-fixed location using portable computing/communications devices such as laptops, notebooks, tablets, smart mobile phones and PDAs. Mobile computing and communications includes, but is not limited to:

- field work
- occasional work from home without a tele-working agreement
- temporary work from a client’s facilities or ongoing work from a client’s premises where the parent agency cannot assure the protective security arrangements, and
- working in transit where the potential for oversight and overhearing is high.

Agencies need to pay close attention to the environment in which workers are expected to operate, as this can range from airport lounges to another agency’s office to a remote community, and may have a significant impact on security requirements.

While agencies may find it hard to implement some elements of protective security in mobile computing and communications arrangements, they need to take all reasonably practicable measures to ensure the safety of mobile employees. Agencies should address any other protective security concerns. See Annex A—Checklist for mobile computing and communications/tele-working.

Most mobile computing locations are Zone One physical security areas. See the PSPF - Australian Government physical security management guidelines—Security zones and risk mitigation control measures. It may not be possible to apply suitable physical security measures to satisfy a higher Security Zone requirement for mobile computing and communications, and agencies should rely on administrative and ICT logical security controls to protect their information and assets. See the Australian Government Information Security Manual (ISM) for logical controls.
3.2 Tele-working

Tele-working provides agencies and employees with flexibility in meeting their objectives by allowing employees to work from alternate fixed locations. Tele-working may also be a strategy in agencies’ business continuity planning.

Tele-work is distinguished from mobile computing by having a controlled environment. Tele-work is subject to a formal agreement between the agency and the employee. Agencies are to treat work from locations that have not received prior approval as mobile computing.

Tele-working includes working away from the office using remote ICT systems in fixed locations such as:

- Working from home on a regular basis, may include based on agency policies:
  - work from home as a normal work arrangement, either full-time or part-time
  - arrangements for staff to regularly work from home outside of normal work hours (day-extender), or
  - under a regular casual tele-working arrangement—for example primary care givers.

- Working from alternative office space:
  - provided on an ongoing basis to the agency in client premises where the agency has some ability to provide protective security
  - provided by the agency in another location—for example business continuity sites or regional sites, or
  - located in another Australian, state or territory government agency’s facilities.

Agencies may wish to supply part-time tele-workers with a dedicated portable device to use in both locations to avoid synchronisation problems and reduce costs. As for part-time tele-workers, day extenders may use a single device. Day extenders, especially senior executives, may have an expectation of agency ICT support at any time, day or night.

As tele-work locations are fixed and in some instances known, there may be additional risks to agency tele-workers, information and assets. Agencies are to assess the protective security requirements of all tele-working locations, including:

- personnel security aftercare
- personal security and safety
- information and ICT security, and
- physical security.

- See Annex A—Checklist for mobile computing and communications/tele-working.

The level of physical security required will depend on the business impact level of any compromise, loss of integrity or unavailability of agency information or physical assets, or the potential for harm to tele-workers, see Sections 4 and 5.

Prior to implementing tele-working arrangements, agencies are to assess the suitability of the protective security measures of any proposed locations where the compromise of official information or assets handled at the location would have a business impact level of high or above. Agencies should assess the suitability of protective security measures in other tele-working locations. See Annex A—Checklist for mobile computing and communications/tele-working.
Most tele-working locations will meet Zone Two physical security requirements without significant modifications to the tele-working site. See PSPF - *Australian Government physical security management guidelines—Security zones and risk mitigation control measures*.

### 3.2.1 Tele-working from home

Tele-working from home is to be subject to a formal agreement between management and the employee. Teleworking agreements normally require an assessment of the home office, or work site. See the [Annex B—Useful Links](#) for links to sites that provide advice on developing tele-work agreements.

Tele-working assessments should assess compliance with any human resources and occupational health and safety (OHS) requirements, and include all relevant security elements as identified in [Protecting agency information and physical assets](#) and Annex A—Checklist for mobile computing and communications/tele-working.

### 3.2.2 Tele-working communications arrangements

Agencies are to include at least the following in any teleworking agreements:

- conditions of employment
- occupational health and safety arrangements, and
- security requirements

The agreement should:

- identify appropriate technology required to access information accessed from the tele-working location—see ISM
- determine what equipment the agency will provide, what equipment the tele-worker will provide, and what will be shared, including any specific controls relating to use of personal equipment
- detail how technical assistance is to be provided in the event of equipment failure or disruption
- determine the physical attributes of the tele-work office and whether they conform to-safety and security standards
- articulate availability expectations—such as, but not limited to, by phone, email
- provide tele-worker emergency procedures, and
- identify procedures to change the agreement.

### 3.3 Working away from the office without ICT support

Working away from the office without ICT support can occur in any of the locations identified for mobile computing and communications or tele-working. The employee may still have access to official information in hard copy and agency physical assets which are to be protected, see [Protecting agency information and physical assets](#).
4. **Personal safety when working out of the office**

Agencies have a responsibility under the *Occupational Health and Safety Act 1991*, OHS Regulations and OHS Code of practice to take all reasonably practicable steps to address any risks, and prevent injury, to their employees, their clients and the public outside of agency facilities as a result of agency actions.

The safety and security of employees should take precedence over security of agency information and assets. Employees should not unreasonably put themselves at risk of injury or harm to protect agency information or assets.

Security advisers and safety officers should work together to develop agency guidelines to assist in reducing risks to staff safety and improving staff security when out of the office. The guidelines could include:

- preventive measures that staff can take prior to leaving the office
- actions to take in an emergency
- dealing with clients and the public (conflict resolution techniques)
- vehicle safety and security
- personal risks when carrying/protecting valuables and attractive agency information and assets, and
- incident reporting procedures.

Additional advice on personal safety is available from Annex B—Useful Links.
5. Protecting agency information and physical assets

Agencies are to:

- assess the risks to Australian Government information and assets
- mitigate the risks to their information and assets to levels acceptable to them, and
- apply controls to give assurance in information and asset sharing arrangements when working away from the office.

5.1 ICT security

Agencies are required to meet all ICT security requirements for tele-working and mobile computing specified in the ISM prior to the commencement of the arrangement.

ICT security for tele-working equipment can be difficult to enforce. When tele-working is performed on agency provided equipment it is reasonable to expect that the equipment will be used in a similar way to ICT equipment located in the agency.

Agencies should clearly define reasonable personal use in their tele-work, and mobile computing and communications policies. There is the potential for agency provided equipment to be used by members of the employee’s family in home-based tele-working arrangements. Agencies should clearly detail any requirements, or restrictions, regarding the use of agency equipment by members of a tele-worker’s family should be included in all home-based tele-work policies.

Mobile, portable computing devices are most at risk from people wishing to steal the equipment for:

- the ‘resale’ value of the equipment, or
- access to the information held on the equipment.

Agencies are required to reduce the risk of unauthorised access to information. The risk of unauthorised access to information is reduced by using robust encryption on mobile computing devices. Agencies are required to apply either:

- encryption as detailed in the ISM for all mobile computing devices, or
- apply all the controls identified in the PSPF - Australian Government physical security management guidelines—Security zones and risk mitigation control measures.

Agencies are to treat as compromised any unencrypted information on a device that is lost. Agencies are to also evaluate the potential for compromise when determining the impact of the loss of any encrypted information.

The principles in the IASF Unclassified Security Awareness Bulletin No. 03/07—Laptop Computer Security, available to ASAs from the Protective Security Policy Community of GovDex, should be applied to all mobile computing devices.

5.1.1 Use of an employee’s personal ICT equipment

Unless agencies can manage the safe disposal or sanitization of an employee’s personal ICT equipment, agencies should not allow the use of personal ICT equipment for processing agency information with a business impact from the compromise of the information of high or above.
Agencies should frequently assess the risks of allowing employees to use personal or private ICT equipment for agency business.

Even when using remote access devices that do not allow agency information to be stored on non-volatile memory of ICT equipment, there is the potential for agency information to be stored on volatile memory of the equipment, see the ISM for details of sanitizing volatile and non-volatile media.

Agencies should also identify to employees that information is written to the volatile memory of ICT equipment when working from a USB stick, or similar device storage device.

For further requirements on the use of personal ICT equipment see the ISM. For additional advice see Annex B—Useful Links.

5.1.2 Use of public ICT equipment, wireless networks and communications

All information accessed on public ICT equipment—for example internet cafes, hotel business centres or airport lounges is at risk. The agency has no control over who can access the equipment, nor the security features or applications enabled on the equipment by its owner or manager.

Agencies are to prohibit employees from accessing security classified information on public computers or other public ICT communication devices.

Agencies should only use Public ICT equipment for unclassified information where there is no alternative and there is a clear, critical business need for the information to be accessed.

5.2 Physical protection of official information when away from the office

Prior to its use, agencies should determine if any work space outside of the office can:

- appropriately secure sensitive or classified information stored at the work area
- the work area be independently secured
- the work area be protected from oversight, or overhearing, by other people, including family and children, and
- the ICT equipment used in the work area be secured or segregated from the agency’s ICT system.

Agencies are to determine their own procedures to ensure appropriate accreditation of proposed sites. This would normally require a security inspection of the proposed sites.

5.2.1 Classified information

Agencies are to prohibit security classified information being stored outside their offices unless the information will be stored in accordance with the PSPF - Australian Government information security management protocol, the Australian Government physical security management protocol and supporting guidelines. This includes the accreditation of any ICT and physical security arrangements.

Agencies should not allow the storage of TOP SECRET information outside of agency premises unless it is critical for an operation. Agencies are required to have ASIO-T4 certification of any storage of TOP SECRET information.
5.2.2 **Business information**

Agencies should determine any specific security requirements for the storage of business information—that is, unclassified information relating to agency business, outside of their premises. This includes information bearing dissemination limiting markers.

Agencies should not allow employees to access business information from tele-centres, public computers or other public ICT communication devices unless there is a critical business reason to do so.

5.2.3 **Conversation security**

Agencies are to develop procedures to protect sensitive or classified offsite conversations from being overheard. It may be impossible to prevent determined adversaries, including foreign intelligence services, from listening to conversations held outside of audio secure areas.

Agencies should only allow classified conversations outside of audio secure areas if it is critical to an operation. Agencies should seek advice from information originators prior to allowing conversations using SECRET information outside of audio secure areas. Agencies are to seek advice from ASIO-T4 and the originating agency prior to allowing conversations using TOP SECRET information outside of audio secure areas.

The following measures may reduce the threat of sensitive conversations being accidentally overheard or recorded:

- Sensitive conversations, including telephone calls, should not be held in hire cars, hotel rooms, or conference rooms unless measures have been taken to ensure audio security. These areas are at high risk of audio surveillance, particularly when travelling overseas.

- Holding sensitive conversations in closed public spaces, whilst sitting or standing in one place, easily allows the conversation to be overheard or recorded. Classified conversations held in public, on aircraft, in airport lounges, whilst at the local café, or other locations known to be frequented by agency personnel are at significant risk and should be discouraged.

- The risk of audio interception is greatly increased when travelling overseas, wherever possible sensitive or classified official information including conversations/telephone calls should be accessed within secured facilities. Allied secure facilities are acceptable, provided they are accredited to the appropriate level and the information being discussed is permitted to be shared with the allied government.

- Where no secure facility is available and a classified conversation/telephone call is essential the employee should find an open public place such as a park or other open area and conduct the conversation while walking, being careful to ensure the conversation is not overheard by casual observers. Parks and open areas offer the greatest protection from casual audio surveillance. ‘White noise’—for example running water such as fountains; may also reduce the ability to remotely record conversations without specialist equipment.

It is much easier to record a conversation than it is to record a laptop's screen. The risk of conducting sensitive conversations in unsecured places is much greater than reading an email or typing a document.

5.2.4 **Physical security of official information in private client facilities**

Agencies can find it difficult to adequately secure their information when their staff are located inside commercial or private client facilities. Agencies will not normally have control over client alarm or keying systems.
Unless agencies have full control over the office space occupied by their staff in client facilities, agencies should treat any non-Australian Government facilities as Zone One areas for information and asset storage.

5.2.5 Options for transferring information to remote locations

It is unrealistic to expect staff to maintain physical custody of the information at all times if it cannot be carried on their person. However, agencies should restrict the use of removable ICT media, such as USB sticks and portable hard-drives, to carry large quantities of information as they are easily lost.

Information is at considerable risk when being transported. Agencies should consider all alternatives prior to giving approval for the transport of information to remote locations by employees. These can include:

- remote secure access to agency ICT networks (if a connection can be arranged)
- transport to nearby Australian Government or jurisdictional facilities by endorsed couriers or secure networks for collection by employees once onsite, and
- storage of the information on a DSD approved portable device that provides additional logical controls to prevent unauthorised access.

Where alternative transport cannot be arranged, agencies should, if possible, make arrangements to secure information during breaks in trips in suitable Australian Government or jurisdictional government facilities.

5.2.6 Disposal of official information

Agencies should have procedures in place for the secure disposal of official information for all working away from the office situations. These procedures should be included in any employee briefing or agreement.

Agencies are to ensure all security classified information is returned to their premises for destruction unless they have approved destruction equipment located off-site.

5.3 Protecting agency assets

Assets are more vulnerable to loss outside of the office environment. An agency should:

- include any assets provided to employees who are working away from the office in the agency’s asset management register, even when the value of the assets is below the threshold normally applied to control agency assets
- only allow employees to remove assets from agency facilities necessary for the performance of their out-of-the-office duties
- assign custody of each asset to individual employees prior to allowing the asset’s removal from agency premises
- advise employees of their responsibilities to safeguard any agency assets for which they have been entrusted, and
- provide employees with incident reporting procedures in the event that assets are lost or damaged.
5.3.1 Portable assets

Most assets that are used by employees out of the office are portable. Once removed from agency premises portable assets are more at risk. These assets can include, but are not limited to:

- vehicles, including plant
- mobile computing devices, including mobile communication devices, see Section 5.1
- security containers and other furniture
- weapons
- animals
- samples—for example biological or chemical samples
- specialist, scientific or research equipment, and
- cultural or collection material.

In addition to any legislative requirements to protect dangerous assets, agencies should:

- advise employees of all measures they are to take to safeguard agency portable assets prior to allowing the assets out of the office
- include a schedule of equipment provided to employees as part of any tele-work agreements, and
- have employees sign for any equipment prior to removing it from agency premises.

Assets should not be left in vehicles that are unattended by agency personnel unless unavoidable or physical security measures are in place to protect the vehicle and its contents.

Assets left in hotel rooms or hotel safes may be at risk, particularly when travelling overseas. The risks to the assets should be evaluated and treated prior to departure.

When travelling, assets in carry-on luggage are usually more secure than checked in baggage, providing the carry-on luggage remains in the employee’s control.

Agencies are to treat as compromised any information contained in lost or stolen physical assets.

5.3.2 Security alarm system options

Agencies should evaluate the need for security alarm systems (SAS) in tele-working arrangements as part of the tele-working risk assessment. If a SAS is required then agencies should use SAS that meet AS 2201.1:2007 Intruder alarm systems Class 2 or above.

Agencies may use portable alarm systems to protect assets in other mobile work situations—for example vehicles may be fitted with alarms and engine immobilisers. Further details are in the PSPF - Australian Government physical security management guidelines—Security Zones and risk mitigation control measures section.

5.3.3 Locating assets in private client facilities

Agencies may not be able to control the security of assets located in client premises, even when given a dedicated work space. Where security cannot be assured, agencies should evaluate the risks to their assets in a similar way to any other unsecure off-site work environment.
Agency assets that are used to regulate the client’s activities may require additional protection where tampering with the assets could compromise the regulation activities.

5.4 Reporting incidents

Where employee safety is at risk the employee should in the first instance, if possible, contact the local police for assistance. Once their safety is assured they are to report the incident to their agency.

Agencies are to have procedures in place for mobile workers to report security incidents. These procedures should include reporting:

- any security incident involving agency information and assets, and
- other incidents at their work location.

Agencies should consider their ability to respond to, and investigate, incidents that occur outside of their premises when developing incident response procedures for mobile workers.

See the PSPF - Australian Government protective security governance guidelines—Reporting incidents and conducting security investigations for further details on agency responsibilities for reporting incidents.
6. **Annex A—Checklist for mobile computing and communications/tele-working**

Australian Government employees are increasingly working away from the office. In each instance of off-site work, agencies are to consider the need to protect official resources prior to any removal of information or assets from the agency’s premises.

The following checklist can assist in assessing the risks associated with any removal and/or use of official resources off-site. Agencies should address any security concerns raised prior to allowing work away from the office or removal of official resources.

- Has the employee been required to read, or been briefed on the requirements for the protection of official resources?
- What is the security classification or sensitivity of the official resources to be removed?
- Why are the official resources being removed off-site?
- How long will the official resources be off-site?
- Have the details of the official resources being removed been recorded?
- Do the official resources being removed belong to another agency? If so, has that agency given its approval?
- How will the official resources be securely transferred or transported?
- Is the removal of the official resources from the agency a temporary/one off or a permanent/long term arrangement?
- How will the official resources be securely stored off-site?
- What is known about the location where the resources are being taken? Is a risk assessment needed in relation to that location?
- What control does the agency have over the security of the location?
- Who has access to the location where the official resources are being stored?
- How will the employee protect his/her work from unwanted scrutiny or unauthorised access?
- How will the employee protect his/her official conversations from being overheard?
- Could the resources being carried reasonably expose the employee to targeting by a foreign intelligence service? Has the employee been appropriately briefed? See *PSPF – Personnel Security - Contact Reporting Guidelines*.
- Is the employee aware of what action he or she is to take in the event official resources are stolen?
- Is the employee considering printing, duplication or disposal of official information in a non-secure environment? What measures have been put in place to ensure official information is not compromised by this activity?
☐ Has the agency authorised the use of any off-site ICT equipment? If so what equipment and in what circumstances?

☐ Does the employee have an authorised email account, or remote ICT access to agency systems, that can be accessed securely?
7. Annex B—Useful Links

7.1 Telework agreements

Telework Australia, a site authorised by the Department for Industry, Innovation, Science and Research under the Telework Awareness Initiative which promotes tele-work. The site provides some useful advice and document templates for tele-work agreements:

- Telework Australia better practice guidelines

7.2 Personal safety

Comcare provides advice on safety in other working environments including:

- driver fatigue
- cash in transit
- FAQs on home-based work, and
- FAQs on work in isolation or remote locations

The jurisdictional police forces provide advice on personal safety, see:

- Queensland Police—Personal safety strategies
- Western Australia Police—Your safety
- Australian Federal Police—ACT policing—Crime and safety
- NSW Police—Personal safety tips

7.3 ICT security standards

The National Institute of Standards and Technology (United States) provides guidance on the technical security of tele-working and mobile computing in their publications:

- Users guide to securing external devices for telework and remote access
- Guide to Enterprise Telework and Remote Access Security
- Security for Telecommuting and Broadband Communications.