AFP National Guideline on information security

View document details (metadata)Close document details (metadata)

Metadata	
Caption	Information security: ICT systems, hardware and software
Document Identifier	NAT18001
Description	This guideline directs systems users to exercise security responsibility to support the security of AFP ICT systems and hardware.
Governance Function	Security
Owned by	Manager Security
Date First Approved	22/12/2017 0:00
Contact Person	s47E(d) @afp.gov.au
Date Published	8/01/2018 0:00
Date Modified	18/9/2019
Date Last Reviewed	22/12/2017
Authorised by	Manager Security
Date of Next Review	22/12/2019
IPS publishing:	Exempt or unsuitable
IPS decision date	22/12/2017 0:00
Instrument Type	National Guideline
Replaces	NAT13055, NAT13056, NAT13057, NAT13059
Stakeholders	Technology & Innovation, Security, Professional Standards

Metadata	
Instrument Classification	UNCLASSIFIED
Dissemination Limiting Marker (DLM)	For official use only
Current SharePoint Version	8.0

1. Disclosure and compliance

This document is marked **FOR OFFICIAL USE ONLY** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the AFP National Guideline on information management.

Compliance

This instrument is part of the AFP's professional standards framework. The AFP Commissioner's Order on Professional Standards (CO2) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the *Australian Federal Police Act 1979* (Cth).

2. Acronyms & definitions

Acronyms and terminologies are defined in the AFP Security Glossary of Terms.

3. Guideline authority

This guideline was issued by Manager Security using power under s. 37(1) of the *Australian Federal Police Act 1979* (Cth) as delegated by the Commissioner under s. 69C of the Act.

4. Introduction

This guideline observes obligations under the:

- Australian Government Information Security Manual
- Australian Government Protective Security Policy Framework
- AFP Commissioner's Order on Security (CO9).

This guideline outlines the obligations for system users relating to the security of AFP ICT systems.

Information security applies to all system users and AFP ICT systems. All system users must protect AFP ICT systems from unauthorised use, including disclosure, modification, manipulation and destruction.

Exception: This guideline **does not** apply to discreet or covert use. For information on discreet or covert use, refer to the AFP National Guideline for official online activities.

5. Policy

The Security portfolio is responsible for the security of all AFP ICT systems, hardware, software and removable data storage devices (RDSDs).

All controls used for the security of AFP ICT systems, ICT hardware, software, RDSDs and system access must be approved by Security.

Prior to implementation, any new business system, application or major modification to an existing business system or application must be reviewed by Security to determine if a risk assessment is required.

When using AFP ICT systems, RDSDs, ICT hardware or software, system users must:

- protect the security and integrity of the systems or item and any information stored
- only access official AFP databases, intelligence and information for the purpose of their official duties and in accordance with legislation
- only use RDSDs, ICT hardware or software for the purposes of their official duties.

System users using the AFP Secret Network (AFPSec) and AFP Top Secret Network (AFPTSN) must comply with governance and separate security documentation available on those systems.

Further information is available on request from Security.

6. Responsibilities

Deputy Commissioners and COO
The Deputy Commissioners and the COO, as appointed system risk owners for major information systems, must make decisions on the acceptance of ICT security risk for the AFP on behalf of the Commissioner.

Chief Information Security Officer (CISO)
The Manager Security (Chief Security Officer) performs this role and is responsible for the strategic direction for security across the AFP. The CISO is also responsible for ensuring the AFP is compliant with national policy, standards, regulations and legislation.

Agency Security Advisor
The Coordinator Physical Security performs this role and provides high-level authority to support the Information Technology Security Advisor in maintaining the physical security of AFP ICT systems.

Information Technology Security Advisor (ITSA)
The Coordinator Information Security performs this role and is the system certification authority. The ITSA may authorise ICT system shutdown, emergency access and access revocation.

The ITSA must advise on ICT systems security to the Security Committee through Manager Security (Chief Security Officer).

System risk owner
A system risk owner is appointed by the Deputy Commissioner Capability and is responsible for ICT security risk of major ICT systems. They are responsible for the system risk acceptance and formal accreditation approval and are the nominated information owner.

The system risk owner may grant waivers for an ICT Security compliance directive in accordance with Commonwealth security requirements.

System risk owners must:

- determine the eligibility criteria and access rights for users of their systems
- delegate authority, if required, to grant access to other system users
- inform Technology & Innovation of delegation details.

System owner
A system owner is responsible for:

- the operation of the system, ensuring it is managed effectively and securely
- delegating the day-to-day management of the system to a system manager.

The system owner is the authority on:

- ensuring the security risk owner has accepted all residual risks
- placing a system into an operational state
- approving the re-assessment of a systems, based on system changes
- terminating a system.

System manager
A system manager is appointed by the Deputy Commissioner Capability to manage, on behalf of the system risk owner, the designated ICT system on a day-to-day basis to ensure the confidentiality, integrity and availability of all information collected, processed and stored on the designated system.

System users
The action of a system user 'logging on' to an AFP ICT system is interpreted as their implicit agreement to comply with the AFP Security governance framework and accept personal responsibility for information security.

AFP appointees with authority to access a third party database/system must ensure they comply with all terms and conditions allocated to that database/system.

Part A – ICT system access

7. Access conditions

The identity and suitability of individuals to access official material must be confirmed before access is granted.

System users must have the following security clearance levels for the below ICT systems:

ICT System	Security Clearance	Compartment Briefings
AFP Core Systems	BASELINE	
AFPSec	NEGATIVE VETTING 1	
CABNET	NEGATIVE VETTING 1	
AFPTSN	POSITIVE VETTING	s47E(d)

For all other systems the minimum security clearance must be determined by the system risk owner.

System users must:

- have a legitimate requirement and authority to access AFP ICT systems
- only be granted access to ICT systems necessary to perform their official duties
- hold a current security clearance appropriate to the highest classification of information stored on, or accessible through, the ICT system they are authorised to use. Refer to the table above and s. 21 below.
- use their own unique logon identifier (user ID) to access an AFP ICT system and be accountable for all actions associated with their user ID
- not allow another person to use a computer account or password not assigned to them
- not attempt to obtain passwords or access computer accounts not assigned to them unless it is part of their official duties
- protect passwords according to the classification of the ICT system or device to which it allows access, refer to s. 7.4 below.

7.1 Access management

Upon meeting the requirements detailed above, access to AFP ICT systems (excluding PROMIS access by non-AFP appointees, refer to s. 7.2 below) must be approved by a system user's supervisor (coordinator or above) unless system specific arrangements are required or have already been approved.

AFP coordinators or above may approve access to personal information held by other system users.

Team leaders or above may approve access to shared resources such as network folders and email distribution lists. Where appropriate and once a supporting business case has been approved by Technology and Innovation (T&I), executive assistants or business administration officers may also approve access to shared resources.

To ensure appropriate use of AFP systems, AFP managers and coordinators should be aware of and monitor system users' information access and activities on AFP ICT systems. Supervisors must ensure system users hold appropriate security clearances and are briefed on the appropriate protective security procedures for handling information.

7.2 PROMIS access by non-AFP appointees

Access to PROMIS by a non-AFP appointee must be endorsed by an AFP manager. Where ongoing access (past 12 months) is required, the sponsoring AFP manager must confirm the ongoing requirement with the system risk owner.

Memorandums of understanding that relate to the access of AFP information systems must incorporate clauses relating to security reporting, personnel and information security requirements and must be reviewed by Security prior to finalisation.

For further information refer to the AFP National Guideline on access to PROMIS by non-AFP appointees.

7.3 Information access requirements

	Certain Sensitive and Compartmented Information [1]	TOP SECRET	SECRET	CONFIDENTIAL	PROTECTED	UNCLASSIFIED with a DISSEMINATION LIMITING MARKER	UNCLASSIFIED
Positive vetting	✓	✓	✓	✓	✓	✓	✓
Negative vetting level 2	✓	✓	✓	✓	✓	✓	✓
Negative vetting level 1	✗	✗	✓	✓	✓	✓	✓
Baseline	✗	✗	✗	✗	✓	✓	✓
Employment screening	✗	✗	✗	✗	✗	✓	✓

Supervisors must notify the system manager, by emailing T&I (ICT-Support) when a system user requires reduced or modified access permissions, including when:

- transferring to different duties
- changing the nature of duties
- on long-term leave of more than 90 days (e.g. long service, maternity or without pay)
- ending a secondment or attachment to the AFP
- ending membership of a joint task force or similar operational team
- suspended from duty
- ending AFP employment or engagement.

Accounts not used for 90 days must be suspended in accordance with T&I procedures.

7.4 Passwords

Passwords must not be written down and kept with any AFP ICT system or mobile electronic device. Where there is a requirement to physically record a password, it must be:

- stored in a sealed envelope which should, at minimum, also contain:
    - the asset number of the device
    - the names of those authorised to use the device
    - the date the password was changed.
- protectively marked to the maximum security classification of the ICT system or device to which it allows access
- handled and stored in accordance with the:
    - level of sensitivity or classification of the information the password protects
    - Access and storage requirements for information and assets
    - AFP Security Governance Framework.

Where a record is kept electronically, for systems up to and including PROTECTED, it should be kept using s47E(d) s47E(d) software, which is available on AFP core systems.

Passwords used to access AFP systems should not be used to access non-AFP systems.

System users must immediately report any password compromise or suspected password compromise to Security by submitting a security incident report or contact Security for advice. The password must be changed as soon as practicable after the incident.

8. Acceptable and prohibited use

8.1 Acceptable use

System users must only:

- use AFP ICT systems in accordance with this guideline and other AFP governance, including:
    - **the need-to-know policy** – system users must only access information needed to perform their official duties and for which they have an appropriate security clearance
    - **information release** restrictions – system users must only release information obtained from AFP ICT systems to another person in accordance with the AFP National Guideline on information management.

System users requiring access to SECRET and TOP SECRET material may be granted an authorised account for the relevant externally provided ICT system. System users must operate third party systems in accordance with the system risk owner's security requirements.

8.2 Limited personal use

Where an AFP ICT system is approved for limited personal use, system users may use it for limited personal use if they comply with all AFP requirements.

Limited personal use must:

- be in accordance with the business area policies and procedures
- not be excessive in cost, space, time or resources
- not affect the ability of AFP ICT systems to operate efficiently
- not require changes to the ICT system or negatively affect security mechanisms
- not fall outside the boundaries of acceptable use
- comply with:
    - AFP Code of Conduct
    - Better Practice Guide on Workplace Bullying and Workplace Discrimination.

8.3 Prohibited use

System users must not, without lawful excuse or authority, use AFP ICT systems:

- in a way that could adversely impact on AFP core business, operational requirements or reputation
- in a way which breaches Commonwealth policies and/or requirements
- for personal gain, including any personal business interest, unless that business interest is approved secondary employment, noting provisions for the Discussion Fora as per s. 10.5 below
- to create, access, distribute or store inappropriate information
- to access non-AFP ICT systems or data that could endanger the security of AFP ICT systems, including:
    - external web-based email (e.g. Hotmail, Yahoo Mail, Gmail)
    - instant messaging
    - seized or intercepted computer data which has not been appropriately sanitised (e.g. electronic evidence)
    - known malicious software or viruses
    - untrustworthy websites or files
    - unapproved ICT hardware
    - file sharing
    - video conferencing.

Where inappropriate material has been unintentionally accessed by legitimate searches, or the nature of material was not evident from the title or link displayed, system users must:

- immediately exit the inappropriate content
- make a file note or diary entry describing the circumstances
- notify their supervisor
- submit an integrity report in accordance with the AFP National Guideline on integrity reporting.

System users, who are required to access inappropriate material for official reasons, on AFP systems not authorised for this use or are outside of their standard duties, must log a PROMIS case note entry or diary note and advise their supervisor for each instance.

9. Internet usage

All system users accessing the internet for AFP business reasons, whether by AFP core systems or any other connection (e.g. stand-alone computers) must ensure their usage does not fall outside the boundaries of acceptable use, including:

- using, without authorisation, any discreet or covert internet connections, as per the AFP National Guideline for official online activities
- being excessive in cost, space, time or resources
- adversely affecting the efficient operation of AFP ICT systems

- on its own, requiring changes to policies or practices, or alterations to security settings
- access to inappropriate material
- compromising the AFP.

Security may block access to specific websites or website categories that may endanger the security of AFP ICT systems or impact the operational availability of AFP ICT systems. Access to a specific website within a blocked category may be authorised on application to Security by the relevant coordinator. For additional information refer to the internet browsing categories, allowed and blocked.

10. Communications

10.1 Telephones and facsimiles

Fax machines transmit information over the public telephone system and must only be used to transmit UNCLASSIFIED information.

The AFPNET telephone system (including facsimiles, mobile telephones, the teleconferencing system and the Voice over Internet Protocol system) and the public telephone system must only be used to transmit UNCLASSIFIED information.

Telephone messaging systems (SMS, MMS, voice mail, pagers and messaging applications) must only be used to transmit UNCLASSIFIED information.

AFP Secret and Top Secret networks have telephone systems that can be used for conversations up to SECRET and TOP SECRET respectively. Refer to s. 27.1 below.

System users must consider who can overhear a telephone conversation, especially in open plan environments.

Travelling with electronic devices

AFP appointees travelling overseas for official purposes must be mindful of the AFP National Guideline on mobile devices. AFP appointees travelling to a country assessed by Security as high risk should only take electronic devices that have not been used prior and will not be used upon returning to country (burn device).

AFP appointee's should contact Security in the first instance, by submitting their signed International Travel Approval Form to Security, to confirm if a burn device is required.

Business areas are responsible for the purchase of burn devices.

For more information on travelling overseas with electronic devices, refer to the Travelling internationally with electronic devices guide and the Mobile electronic devices returning from travel FAQs.

10.2 Wireless communication devices

System users must not connect any wireless communication device to any AFP ICT system or network until approval to operate that device has been received from the system risk owner after consultation with Security.

10.3 Email

System users must treat unsolicited emails (spam) as if they contain inappropriate material and must not reply or forward:

- chain emails
- junk email
- games
- non-work related advertising.

System users must:

- not use **personal email accounts** to send or receive official information obtained in the performance of their AFP duties
- comply with the information security articles and FAQs on security classifications of email allowed to organisations**.** Adding an external email address to AFP mailing lists is at the discretion of the mailing list owner.
- only send information (including attachments) classified:
    - FOR OFFICIAL USE ONLY or above to recipients authorised to receive information of that classification.
    - SECRET or TOP SECRET from the AFP Secret or Top Secret networks respectively.
    - Sensitive: Cabinet via CABNET.
- only **automatically forward emails** if it is:
    - appropriate to do so (e.g. the recipient has a 'need to know')
    - restricted to an AFP email address.
- limit **out-of-office email notification** to respond to internal recipients only, as these notifications also respond to spam
- not add AFP email addresses to **external mailing lists** of non-government organisations unless it is required for official purposes, such as registering for a conference
- not use AFP core system passwords when using an AFP email address to register online for official purposes.

System users who are contractors must list their position in the signature block of their AFP email as contractor.

10.4. Social networking

System users:

- should not identify their employment with the AFP in unofficial online social networking (this includes the use of AFP logos and insignia)
- should act responsibly and mitigate risks to their safety
- must not:
    - establish a personal account with an AFP email address
    - compromise the AFP's security, reputation or operational effectiveness
    - use AFP logos or insignia for private purposes
    - breach s. 60A of the *Australian Federal Police Act 1979* (Cth).

System users and their supervisors must ensure:

- the use of social networking via personal devices whilst on duty is reasonable as per s. 8.2 above
- their usage of social networking sites on AFP ICT systems does not fall outside the boundaries of acceptable use, in accordance with s. 8.1 above.

Any use of AFP logos and insignia must be in accordance with the AFP National Guideline on intellectual property, commercialisation, logos and insignia.

For further information refer to the AFP National Guideline on social media (drafting) or contact the Social Media team.

10.5. Discussion Fora use

System users may use the AFP Discussion Fora for general internal interactive discussion on matters of broad interest or relevance. The AFP Discussion Fora facilities must only be used for AFP-related or AFP-approved purposes, including:

- AFP business

- professional, competency and organisational development and technical literacy
- AFP-sanctioned social activities
- activities which benefit or support charitable work or the AFP's role or presence within the community
- other non-official information relevant to the interests and support of the AFP and AFP personnel within the work environment
- the reasonable sale of personal items (via the Employee Forum) that complies with all other AFP governance requirements and does not include commercial sales (e.g. multi-level marketing or connection to a business interest)
- advertising approved secondary employment business, goods and services (via the Blue Pages).

The use of AFP Discussion Fora facilities must be consistent with the AFP Core Values, as per the AFP Commissioner's Order on Professional Standards (CO2).

Reasonable sale of personal items refers to advertising a moderate quantity of items belonging to a system user that a sensible person would:

- not find to be extreme or excessive
- not associate with a conflict of interest
- find in keeping with relevant governance on using information and communications technology, and does not detract from the system user's AFP duties.

Classified information must not be posted on the AFP Discussion Fora.

The AFP reserves the right to moderate any material posted on the Discussion Fora.

The Commissioner or their delegate, as per AFP Commissioners Order on security (CO9) may authorise the removal of any posting it considers inappropriate or out of date.

11. Printer security

System users must:

- not leave sensitive or protectively marked information on printers
- ensure unmanaged printers with wired or wireless connections (including Wi-Fi and Bluetooth) are not connected to any AFP equipment
- ensure all expired printer cartridges and consumables are sanitised prior to disposal
- sanitise printer cartridges and consumables that are relocating to a less secure area.

For information on sanitisation, refer to the How to Sanitise AFPNet Printer.

Secret systems installed outside of a Zone 5 area must not have printers connected, unless authorised in writing by Manager Security (Chief Security Officer) on advice from the Information Technology Security Advisor. In these instances, business areas must establish ongoing and effective procedures for the accountability of each printed document in accordance with Attachment 3 – Classified documents accountability.

System users printing from the AFP Secret Network and AFP Top Secret Network must comply with governance and separate security documentation, available on the systems or from Security.

12. Software

System users must maintain the confidentiality, integrity and copyright of software, whether it has been developed by the AFP or purchased commercially.

System users must not download any software from the internet. **Exceptions** to this include:

- for discreet or covert use; however, all downloads must be done from a reliable source
- applications downloaded from a reliable source to AFP-approved mobile phone or tablet computers.

To purchase software system users must contact the Technology & Innovation portfolio in accordance with the AFP National Guideline on procurement and contracting.

Overt system users who have an approved business requirement to have software downloaded must submit a request to Technology & Innovation (via ICT-Support) with the location of the file and a description of the business requirement. Failure to do so may result in the software not functioning on AFP ICT systems.

For further information contact Security.

13. Removable data storage devices and ICT hardware

Privately owned or unapproved ICT hardware must not be:

- connected to any AFP ICT system or network
- used to process or store official or classified information.

System users must purchase approved RDSDs and all overt ICT hardware through the Technology & Innovation portfolio in accordance with the AFP National Guideline on procurement and contracting.

All leased official hardware that can store information must include provisions to sanitise or destroy the data at the end of its lease. Further information is available on request from Security.

For information regarding the procurement of ICT hardware for discreet or covert use, refer to the AFP National Guideline for official online activities.

Information regarding approved RDSDs is available at the Removal data storage devices FAQs.

13.1. Handling and storage

All overt ICT hardware must be registered, issued, receipted, disposed of and accounted for in accordance with AFP asset management guidance.

System users must:

- when storing official information on an RDSD, only use an approved RDSD
- ensure RDSDs and ICT hardware used for the processing or storage of classified information are:
    - not shared with, or loaned to, anyone who does not have the necessary need-to-know and the required security clearance
    - appropriately sanitised (if previously used), as per s. 23.5 below, before transferring information to another organisation, area or individual.
- ensure approval is granted, and an audit trail recorded, before moving information outside the AFP's secure or authorised work area in accordance with the AFP National Guideline on information management
- be appointed by the system risk owner as an authorised user in order to download data from AFP core systems to CDs or DVDs (downloading data permissions must be administered by the AFP Technology & Innovation function)
- minimise the risk of compromise to information by deleting information on RDSDs when it is no longer required
- ensure the safe custody of any RDSD or ICT hardware under their control until it is formally transferred to another system user or returned to the issuing authority
- ensure passwords and/or security authenticators are kept separate from the respective ICT hardware
- comply with separate specific requirements regarding the use of RDSDs and the removal of information on secret and top secret systems.

For information on the management and control of ICT hardware used for the purposes of covert or discreet activities, refer to the AFP National Guideline for official online activities.

14. Mobile computing

System users must:

- only use AFP issued, owned and configured devices for mobile computing
- only connect remotely to AFP core systems per s. 14.1 below
- only store information classified up to and including PROTECTED on an approved AFP portable device
- not store CABINET or Security-Caveated material, or information classified CONFIDENTIAL or SECRET on a mobile device unless approved by the Manager Security (Chief Security Officer)
- not store TOP SECRET information on a mobile device.

System users using mobile computing devices must only use RDSDs that are approved for the storage of information. These devices must be equipped with approved security controls.

14.1 Remote access

System users must only access ICT systems remotely if:

- it is necessary for system user to perform their duties
- it is via AFP owned, configured and approved ICT systems
- the connections are secured per security controls certified by the ITSA
- there is a two-factor authentication process available
- tokens (hard or soft) are allocated
- through a method risk assessed and approved by Security (i.e. using SatinLOW).

To obtain privileged or remote access to the AFP Secret Network or AFP Top Secret Network systems, system users must receive approval from the network owning agency.

15. Monitoring AFP ICT systems

System users must be aware that the AFP reserves the right to audit and remove any unauthorised material from its ICT systems without notice.

All system users' access to, and activities on, AFP ICT systems are continuously monitored and recorded by Security and Technology & Innovation to:

- ensure compliance with this and other governance
- ensure the integrity of information contained within AFP's ICT systems is maintained
- investigate conduct that may be illegal or adversely affect the AFP or its appointees
- detect inappropriate or excessive personal use
- monitor security.

Use of AFP ICT systems is monitored through an individual's unique logon identifier (User ID) and access rights governed by a password personal to that user.

Requests for audits of ICT systems must be approved by a coordinator or above, or team leader for Professional Standards or Security, and forwarded to Security.

Part B – Security of ICT systems and access

16. Accreditation of AFP ICT systems

All AFP ICT systems must be security assessed and accredited by the AFP's accreditation authority, as per the AFP Commissioner's Order on Security (CO9) and the AFP ICT System Accreditation Plan.

Externally provided ICT systems deployed within the AFP are subject to security assessment and possible accreditation as national security systems.

17. Audit of AFP ICT systems

All AFP ICT systems must have an audit capability to meet the AFP's security requirements.

Prior to the development or implementation of any new AFP ICT system, consultation must take place with Security to ensure the provision of compliant system security monitoring, audit logging and related tools to enable the effective monitoring and reporting of AFP system activities.

Where new ICT systems are unable to be audited by existing security tools, the provision of a suitable audit and monitoring capability must be included in consultation with Security.

Where applicable, all existing AFP ICT systems must perform the level of audit logging and security monitoring as per the Security ICT system audit plan. Where proprietary systems, devices or tools exist to enable the monitoring of these systems, provision for access to these logs must be made available to Security.

System and application security and audit logs should clearly identify which platform, system or application the logs are associated with, particularly in the case of an ICT system having multiple environment instances. All audit logs must be protected in accordance with AFP security standards. Further information is available on request from Security.

18. Data retention

Data on ICT systems must be retained online in accordance with the system risk owner requirements for availability and accessibility of data. Data retention requirements are also subject to the *Archives Act 1983* (Cth).

19. Monitoring AFP ICT systems

All activities on AFP ICT systems must be monitored by Security and Technology & Innovation.

All AFP ICT system access grants, modifications and revocations must be recorded (logged) by the Technology & Innovation portfolio for auditing and denial purposes.

20. Access Conditions

20.1 Shared, service and test accounts

Shared, service and test account usage must:

- for shared accounts, be approved by the area coordinator or above and all approval records kept for auditing
- for service and test accounts, be approved by a Technology and Innovation (T&I) coordinator or above and all approval records kept for auditing
- be listed in an auditable format/ICT system and reviewed every 6 months by a member of T&I at the level of coordinator or above
- have an appointed owner to be accountable for actions
- use account names that conform to naming standards so they are easily identifiable
- use passwords as per existing policy, except that:
    - shared test accounts may have a password expiry of up to 6 months
    - service account passwords must be reset every 6 months or when an individual who has privileged access is no longer an authorised user of the shared account.

Shared test accounts must not be:

- used if an individual test account is available
- able to access both production data and test data.

Where shared accounts are required for shared equipment used in meeting rooms, these accounts must not have access to AFP core systems classified information resources, including shared drives, SPOKES, PROMIS and email.

20.2 Privileged access

Privileged access must only be provided to AFP appointees who have both an:

- approved business need to maintain AFP ICT systems
- appropriate security clearance.

Privileged access to T&I managed systems must only be authorised by a T&I coordinator or above. Authorisation must be recorded within a system which allows subsequent auditing.

Privileged access to any ICT system not managed by the T&I portfolio must only be authorised by the system manager or their delegate. Authorisation must be recorded within a system which allows subsequent auditing.

Privileged access accounts must not be used:

- remotely where a two-factor authentication process is not available
- as a primary or daily logon account
- as an automated method to bypass security controls without the approval of the Information Technology Security Advisor (ITSA)
- to access internet sites
- to download/upload files from the internet without the approval of the ITSA
- to send or receive emails externally without the approval of the ITSA.

21. Security classification of AFP ICT systems

All AFP ICT systems are classified by the system risk owner according to the highest level of classified data processed on the system.

Information must only be processed, stored or transmitted on ICT systems that are approved for its security classification. Refer to the below table:

ICT System	**Highest Classification Allowed**	**Other Restrictions**
AFP Core Systems	PROTECTED	No security caveats (unless in draft format) No cabinet-related material (unless in draft format)
AFPSec	SECRET	No cabinet-related material
CABNET*	SECRET Sensitive: Cabinet	
AFPTSN	TOP SECRET	No cabinet-related material

*** Note:** In accordance with the Australian Government Cabinet Guideline information classified with the DLM of Sensitive: Cabinet must hold a minimum classification of PROTECTED and **must only be held on a Cabinet system**.

Prior to endorsing applications for system access by system users, supervisors must consider the access conditions and enforce the required security clearance levels, per s. 7 above.

22. Support of ICT systems

The system manager must ensure suitable security controls are implemented for all ICT systems under their control. These controls include:

- physical security
- restricted system access by administrators and system users
- secure transfer of information.

All ICT systems, including cloud based/external provider must be held within accredited facilities, as per the PSPF – Australian Government Physical Security Management Protocol and supporting guidelines:

ICT System	Accredited Zone
AFP Core Systems	Zone 3
AFPSec	Zone 4
CABNET*	Zone 4
AFPTSN	SCIF

The system risk owner must:

- ensure ICT systems are certified by the appropriate authority (contact AFP Security for assistance)
- not establish standalone systems to process or store information classified SECRET or TOP SECRET without written authorisation from the ITSA
- ensure unmanaged ICT systems are not held in a Zone 5 area or SCIF without the approval of the ITSA.

Any exemptions for security controls must be discussed with Security and if necessary approval obtained from the system risk owner.

22.1. Cloud services

The AFP must, where it is fit for purpose, adopt cloud-based services that provide adequate protection of data and delivers value for money.

Prior to any acquisitions or integration of a cloud-based service, business areas must submit a completed security risk assessment to T&I (via ICT-Support).

Cloud-based services must be in accordance with:

- Australian Government Cloud Computing Policy
- Australian Government Information Security Manual (ISM)
- Australian Government Protective Security Policy Framework (PSPF)
- Australian Privacy Principles (Privacy Act).

22.2 Connecting external systems to AFP systems

System users must not allow any external or foreign ICT system to be connected to AFP ICT systems without obtaining prior approval from Security.

22.3. Hacking or searching information security mechanisms

System users must not search security mechanisms of ICT systems (including external websites) without lawful authority.

System users with lawful authority must only probe security mechanisms using ICT systems approved to do so.

System users must not probe security mechanisms of AFP ICT systems without written approval from all of the following:

- ITSA
- system risk owner
- system manager.

22.4 Screen locks

All AFP ICT system access terminals (desktops/laptops) must have automatic screen and session locks enabled.

Where a requirement exists to have an account without a screen lock, it must be configured in accordance with the 'Shared, service and test accounts' requirements, as per s. 20.1 above.

23. Security of RDSDs, ICT hardware and software

All controls used for the security of ICT hardware and RDSDs must be approved by Security.

ICT security hardware and software must be assessed by Security prior to their use within the AFP ICT environment.

All RDSDs and ICT hardware containing storage media which has been used to store or process information must only be transferred, exchanged or disposed of in accordance with this section.

23.1 Purchasing ICT security hardware and software

All overt ICT hardware or software to be used within the AFP to provide security functionality must be approved by Security prior to being purchased.

For information regarding the procurement of ICT hardware for discreet or covert use, refer to the AFP National Guideline for official online activities.

23.2 Repair and maintenance

ICT hardware used for processing classified data must always be inspected and/or repaired by a suitably cleared T&I AFP appointee, service agent or supervised un-cleared service agent.

Service agents must be supervised at all times by an appropriately cleared T&I AFP appointee while working on ICT hardware.

System users removing ICT hardware from AFP controlled premises for maintenance or repair must ensure all media is removed or appropriately sanitised prior.

Where it is impracticable to remove or sanitise the media from ICT hardware, system users must seek advice from Security and undertake any actions recommended in accordance with that advice, prior to removing the hardware from AFP premises.

23.3 Removal from AFP premises

ICT security hardware and ICT hardware must not be removed from AFP premises without written approval from the respective coordinator or above.

Note: Approval is not required for the removal of AFP approved and issued mobile computing devices and portable ICT equipment from AFP premises.

Where there is a requirement to process or have access to information outside of AFP controlled facilities, system users must only use AFP owned and managed ICT hardware, unless approved by Security.

System users authorised to remove ICT security hardware or ICT hardware from AFP premises must:

- ensure the appropriate level of physical protection of the hardware at all times whilst outside AFP premises
- comply with the:

- AFP National Guideline on information management
- Attachment 2 – Transferring and transporting classified information
- Australian Government Protective Security Policy Framework
- Australian Government Information Security Manual.

23.4 Transfer

Before re-allocation or transfer of RDSDs or ICT hardware to another system user, workgroup or team, any media containing information classified up to and including PROTECTED must be sanitised by a method approved by Security.

Any media containing, or which previously contained, information classified CONFIDENTIAL or above, must:

- not be transferred
- be destroyed by a method approved by Security.

23.5 Sanitisation

To remove all information from RDSDs or unserviceable storage devices system users must follow the approved sanitisation procedures.

For information on sanitising, refer to the media sanitisation section of the Information Security Manual.

Where RDSDs cannot be sanitised or when there is no requirement to keep them, system users must contact T&I (ICT-Support) to arrange sanitisation and/or destruction of the equipment.

23.6 Disposal/part exchange

ICT hardware used for processing information classified up to and including PROTECTED must not be offered for disposal or part exchange outside the AFP unless the hard disks or storage media have been either:

- replaced
- securely sanitised or destroyed by a method approved by Security.

ICT hardware used for processing information classified as CONFIDENTIAL, SECRET or TOP SECRET must not be offered for disposal or part exchange outside the AFP unless the hard disks have been either:

- replaced
- securely destroyed by a method approved by Security.

Part C - Zone 5 areas and SCIFs

24. Access to ICT systems in a Zone 5 area or SCIF

24.1 New user accounts

When a new user account for a Top Secret ICT system is required, the following procedure applies:

- An AFPTSN application form, available via AFP Corporate Forms and Templates (Part 1), and from local vaults (Part 2) must be completed and supplied to T&I (ICT-Support), along with a copy of an iAspire TSE completion certificate.
- The ICT system administrator must ensure all details are correct prior to forwarding Part 2 of the request forms to the host agency for account creation.
- The relevant Top Secret Control Officer (TSCO) should provide the user with:
    - all relevant security documentation
    - a verbal brief outlining the user's responsibilities.

24.2 Account closure

When a user account is no longer required, the following procedure applies:

- the user must notify their TSCO and the Communications Security Officer (COMSO) of the date and reason to close the account
- the TSCO must notify the system administrator to suspend the account
- COMSO must:
    - administer compartment debriefings as required
    - notify the system administrator to finalise the user's account form.
- the system administrator must close the account and retain all parts of the account for auditing purposes.

25. ICT Equipment

25.1 Information communications and technology (ICT) equipment

All ICT equipment other than AFP approved laptops and mobile devices must be held within accredited facilities, as per the PSPF – Australian Government Physical Security Management Protocol and supporting guidelines.

25.2 Repairs to ICT equipment

AFP ICT equipment classified SECRET (located in a Zone 5 area or SCIF) or TOP SECRET (located in a SCIF) must only be installed, repaired or configured by appropriately qualified, authorised and security cleared AFP appointees.

AFP ICT equipment classified up to PROTECTED and located in a Zone 5 area or SCIF may be repaired or configured by T&I personnel who:

- possess a Negative Vetting 1 security clearance
- remain under the supervision of an appropriately cleared and briefed AFP appointee of the area or the TSCO.

For visitor control procedures, refer to the National Guideline on physical security (drafting).

The installation, repair and configuration of third party ICT equipment (not AFP Secret Network or AFP Top Secret Network systems) located in a Zone 5 area or SCIF must comply with the owning agency's System Security Plan requirements which are provided at the time of installation by the owning agency (can be obtained from Security).

26. Information Management

AFP managers must adequately provide for the protection of classified material in security plans relating to their activities. All information held by the AFP must be:

- classified in accordance with the Better Practice Guide on applying protective marking and the Business Impact Levels
- stored in accordance with the access and storage requirements for information and assets
- transferred and transported in accordance with Attachment 2 of this guideline
- recorded in a classified documents register (refer to Attachment 3 –classified document accountability) where classed as accountable material
- managed in accordance with the AFP National Guideline on information management
- for registry files, accurately recorded in PROMIS and returned to the Records Management Unit when no longer required. AFP appointees transferring areas must ensure the files are transferred correctly and PROMIS updated to reflect the new file holder.

Sensitive compartmented information (SCI) must only be stored, handled, discussed and/or processed (electronic or otherwise) in a facility accredited by the Australian Signals Directorate Defence Intelligence Security to be a SCIF.

Information classified TOP SECRET must be processed electronically in a SCIF, but may be stored, handled and discussed in a Zone 5.

26.1 Classified documents accountability

Classified Documents Registers (CDRs) must be used to record the receipt, storage, physical transmission, disposal and destruction of all accountable material.

Where a business area handles documents of different classifications, a separate CDR must be maintained for Sensitive: Cabinet, TOP SECRET and codeword documents. Documents marked with security caveats do not require a separate CDR.

While it is not a requirement, information classified PROTECTED may be recorded in a CDR to maintain strict control over the classified material.

26.2 CDR responsibilities

CDR supervising member (CDRSM)

Line managers responsible for business areas that handle accountable material must appoint a CDRSM(s).

Prior to being appointed as a CDRSM, individuals must:

- be an AFP appointee
- hold a current AFP security clearance (without restrictions) to the level of the documents being handled
- have received training from the COMSO in the maintenance of a CDR
- demonstrate a high order understanding and commitment to safeguard and account for the material held.

The CDRSM for TOP SECRET and codeword documents should be the relevant Top Secret Control Officer. The CDRSM of a Zone 5 area or a SCIF must conduct a monthly audit of a progressive 10% sample of the complete CDR document holdings.

The CDRSM must be recorded on the opening page of the CDR.

CDR maintaining member (CDRMM)

All AFP appointees who notate classified documents in their area's CDRs are the CDRMMs and must be recorded on the opening page of the CDR.

CDRMMs are responsible for:

- recording documents within the CDR and the daily maintenance of the register
- ensuring safe-hand receipts for transmitted documents are returned, as per Attachment 3 of this guideline
- notifying Security of lost documents by submitting a security incident report.

CDRMMs must:

- properly receipt, account for and record the disposal, transfer or removal of each separate copy of the item, by use of a CDR
- only use the AFP approved form of CDR (AFP Form 819), which can be obtained from the Communications Security Team (no electronic CDR form is endorsed for use in AFP)
- appropriately classify a CDR – CDRs must be classified on their content, not on the documents they record. If care is taken not to identify nationally classified material in the document title, it should rarely be necessary to classify the register above FOR OFFICIAL USE ONLY
- store CDRs separately from the material it records and also in accordance with the requirements for its own classification
- use, transfer, retain, archive, close and dispose of a CDR in accordance with Attachment 3 of this guideline.

Communications Intelligence Security Officer (COMSO)

The COMSO must:

- manage the issue of all CDRs
- maintain a master record of all open and closed registers
- annually conduct a 100% audit of CDRs (calendar year).

For the appropriate use and management of a CDR see Attachment 3 of this guideline.

26.3 Sensitive compartmented information

Sensitive compartmented information (SCI) must only be stored, handled, discussed and/or processed (electronic or otherwise) in a facility accredited by the Australian Signals Directorate Defence Intelligence Security to be a SCIF. SCIFs comprise those facilities listed at access and storage requirements for information and assets.

AFP appointees must not be provided with access to SCI unless:

- the position they occupy is listed on the AFP designated security assessment position register and they have a need to know
- they have received the appropriate compartment brief from the relevant agency, as below
- they have signed the corresponding briefing acknowledgement forms
- the information is received within a SCIF
- they have undertaken a SCIF familiarisation tour conducted by the relevant Top Secret Control Officer or the COMSO.

Compartment briefs

Supervisors of AFP personnel requiring compartment briefs must arrange the briefings through the Communications Intelligence Security Officer (COMSO). AFP personnel must not directly approach external agencies to arrange their own briefings.

When access to a compartment is no longer required, AFP appointees must arrange for the COMSO to formally debrief them. AFP appointees who supervise or otherwise work with other AFP personnel must ensure those AFP personnel who no longer require access to a compartment are formally debriefed by the COMSO.

26.4 Communications intelligence material

AFP appointees who handle communications intelligence (COMINT) material must ensure that:

- they comply with:
    - the AFP National Guideline on information management
    - all COMINT security instructions held in the s7(2) s7(2) A copy can be found on the s47E(d) s47E(d)
- they have been given the necessary briefings
- records are maintained for the handling, printing, movement and destruction of all COMINT material within the AFP via the appropriate classified documents register
- the printing of material is strictly controlled and all copies must be:
    - accounted for in a CDR
    - destroyed (using an 'A' Class Shredder) after 14 days. If material is required for a longer period, approval must be sought from the originating author, business unit or agency.
- they do not reproduce COMINT material unless approved by the originating author, business unit or agency