AFP National Guideline on software management and copyright

1. Disclosure and compliance

This document is classified **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 the disclosure of information.

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

AFP	Australian Federal Police
AFPHUB	Australian Federal Police Hub
AFPNET	Australian Federal Police Network
CFI	Commissioner's Financial Instruction
CIO	Chief Information Officer
GST	Goods and Services Tax
ICT	Information and Communications Technology
LAN	Local Area Network
WAN	Wide Area Network

3. Definitions

Appointee – is defined by s. 4 of the *Australian Federal Police Act 1979* (Cth).

AFP computing facilities – are information and communications technology (ICT) systems:

- owned or leased by the AFP

- operated on behalf of the AFP by contractors or consultants
- on which AFP data is processed
- including networks, stand-alone computers and privately owned computers authorised to process AFP official data.

AFPNET – is AFP's corporate ICT System

Computer program – is a set of statements or instructions to be used directly or indirectly by a computer to bring about a certain result.

Content – is data that can be displayed by a computer, such as text, sound, images, photographs and films.

Copyright – is a legal protection for authors of original works, providing exclusive rights to reproduce these works and to control the various ways in which the works may be disseminated. These rights prevent unauthorised copying, adaptation, distribution, rental, public performance and public display of the author's original works (including 'Software', 'Computer programs' and 'Content'). Copyright law in Australia is governed by the *Copyright Act 1968* (Cth).

Free software – is 'software libre' or 'libre software' that can be:

- used, studied, and modified without restriction
- copied and redistributed in modified or unmodified form
- obtained usually without cost.

Freeware – is copyrighted computer software licensed to be available to use free of charge for an unlimited time.

Hardware – is the physical electronic components of an ICT system, including peripherals (e.g. monitors, keyboards, printers, external hard disk drives, routers, encryption devices etc.).

Illegal software – is Software that is unlicensed.

Information technology – is the technology to acquire, store, process and distribute information by electronic means, including radio, television, telephone and computers.

Information Technology Infrastructure Library – is better practice guidance for ICT service management developed by the Office of Government Commerce (UK). It is widely accepted internationally.

Infringement – means, in relation to Copyright, compromising the exclusive rights of the Copyright owner by making a copy or adapting (or authorising the reproduction or adaptation of) the work (Computer program, Software or Content) without the permission of the Copyright owner.

Infringing copy– means a copy of the work (Computer program, Software or Content) made which compromises the exclusive rights of Copyright owners outlined in s. 31 of the *Copyright Act 1968* (Cth) (see s. 36 of the *Copyright Act 1968* (Cth)).

ICT system – includes terms 'ICT system' and 'system' and both mean an electronic based system incorporating hardware and software to process information. Such systems may be used, for example, for word-processing, databases, data exchange, telephone interception, data

communications, management support, etc.

Major ICT system – includes mid-range systems, LANs, WANs and communications links or networks.

Privately owned content – is content not owned by the AFP but owned by AFP appointees or where AFP appointees hold the copyright or distribution rights.

Public domain content - is content not owned or controlled by anyone and is considered 'public property' and available for anyone to use for any purpose.

Shareware – is software obtainable free of charge to try out (usually for a limited time) a program before the full version of the program is purchased.

Software – is a set of computer programs used to make content available to the user.

System – means an ICT system defined above.

System owner – is a senior AFP appointee responsible for managing (and the security of) a designated ICT system.

System users – are any persons specifically authorised to access AFP ICT systems.

Unauthorised software – is software not approved by the CIO for use on AFP ICT systems managed by ICT.

4. Guideline authority

This guideline was issued by the Chief Information Officer 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.

5. Introduction

This guideline outlines the policies, procedures and responsibilities to prevent infringing software copyrights and properly manage AFP software assets.

6. Legislation

The *Copyright Act 1968* (Cth) ('the Act') sets out how Copyright applies for material created both before and after 1968. Under the Act, Computer programs are protected as 'literary works', like novels or poems.

Part V Division 5 Offences and Summary Proceedings of the Act sets out a range of offences relating to copying a work (Computer program, Software or Content) or otherwise compromising the exclusive rights of a copyright owner with the intention of obtaining a commercial advantage or profit or for any other purpose that has a substantial prejudicial impact on the copyright owner if the Appointee knows, ought reasonably to know, or is negligent to the fact that the copy or related conduct infringes Copyright.

Generally, Appointees must ensure their Software use is lawful and does not, for example,

constitute:

- copying Software or accompanying documentation (e.g. manuals), without the Copyright owner's permission;
- knowingly distributing infringing copies of Software;
- running a copyrighted Computer program on 2 or more computers simultaneously unless the licence agreement specifically allow this (that is, a multi-user or site licence);
- making unauthorised (infringing) copies of Software because a senior officer, colleague or friend requests or compels it;
- importing Software into Australia for commercial purposes without Copyright owner permission;
- distributing Software imported into Australia without Copyright owner permission; or
- loaning software so an infringing copy can be made, or making an infringing copy while it is on loan.

A defence relating to law enforcement and national security is provided in relation to some offences, whereby the offence does not apply in respect of anything lawfully done for the purposes of law enforcement or national security by or on behalf of the Commonwealth or a State or Territory. If in doubt, please refer such matters to AFP Legal for further assistance.

7. AFP software asset management policy

The AFP respects and adheres to all computer software copyright and the terms of all software licences to which the AFP is a party. The AFP also manages its software assets and ensures it installs and uses only legal software on its computers (including portables) and servers.

The AFP will take all reasonable steps to prevent system users of AFP computing facilities from duplicating licensed software or related documentation to use on AFP premises or elsewhere unless the AFP is expressly authorised to do so by the copyright owner. Unauthorised software duplication may subject system users and/or the AFP to civil actions and/or criminal penalties under the *Copyright Act 1968* (Cth).

Appointees must not use software inconsistently with its applicable licence agreement, including giving to or receiving software from clients, colleagues, contractors, etc.

AFP appointees must acquire, copy, distribute, transmit and use software in accordance with this guideline and the terms and conditions of any licence agreement accompanying a particular software product.

The AFP Code of Software Ethics is Attachment 1 of this guideline.

8. Responsibilities

8.1 Chief Information Officer

The Chief Information Officer has overall responsibility to implement and enforce the policies and procedures in this guideline. ICT must develop and implement a software management and compliance program based on the policy and procedures in this guideline in respect of ICT systems and services delivered and managed by Information and Communications Technology (ICT).

8.2 ICT system owners and AFP supervisors

ICT system owners, National Managers, Managers, Coordinators and team leaders are responsible for aspects of software management and compliance directly related to ICT systems and/or their functional areas, work groups or teams. In particular, they must ensure access to legitimate software is provided to system users who need it.

8.3 System owners of non-ICT managed systems

Owners of AFP ICT systems not managed by ICT must implement and enforce the policy and procedures in this guideline in respect of systems, including developing a software management and compliance program and assessment of risks associated with the product.

8.4 ICT software manager

The ICT software manager must coordinate the ICT software management and compliance program in respect of ICT systems managed by ICT (e.g. AFPNET, AFPSec, SAP, RADARS, AFPHUB etc.).

8.5 System users

System users must maintain software confidentiality, integrity and copyright, whether it was developed by the AFP or purchased commercially. In particular, system users must:

- use software in accordance with licence agreements
- not make, without appropriate authority, copies of AFP owned or leased software for work related or personal purposes
- not remove, without appropriate authority, AFP owned or leased software from AFP controlled premises
- not give, without reasonable excuse, copies of AFP owned or leased software to persons outside of the AFP
- report all instances of software misuse.

9. AFP approved software

Major AFP ICT systems must only use commercial and/or AFP-developed software that has been evaluated and tested in accordance with guidelines issued by ICT or otherwise approved by the CIO.

9.1 Software assessment

All software, for ICT managed systems acquired by the AFP must undergo an ICT Security Assessment to identify any security risks prior to installation. ICT Security will then recommend additional controls, if necessary. A security assessment waiver can only be approved by the ICT Security Advisor.

All newly acquired software must also be assessed by relevant areas of ICT facilitated thorough the ICT Support Centre, to ensure compatibility with AFP ICT systems.

A register of approved software and applicable controls will be maintained on the AFPHUB - Approved Software List.

9.2 Access to software

The AFP will provide system users with access to legitimate copies of AFP approved software necessary to perform their official duties.

9.3 Illegal or unauthorised software

Illegal or unauthorised software must not be installed onto an AFP ICT system without first obtaining CIO approval. An appropriate authority must also first analyse and examine it and determine if there is a legitimate operational requirement to install it.

10. Copyrighted content

Content must not be stored or used on AFP ICT Systems without prior approval from the CIO, unless either

- specifically copyrighted to the AFP
- the copyright owner's permission has been sought and granted.

10.1 Access to copyrighted content

The AFP must provide system users with access to legitimate copies of AFP approved content necessary to perform their official duties.

10.2 Public domain and privately owned content

Unless specifically authorised by the CIO, public domain or privately owned content must not be installed or used on AFP ICT systems.

10.3 Illegal or unauthorised content

Illegal or unauthorised content must not be installed on an AFP ICT system without:

- first obtaining CIO approval
- an appropriate authority having analysed and examined and determined it is a legitimate operational requirement to install it.

11. Software asset management

11.1 Software procurement

Unless otherwise agreed by the CIO,
requests for software, including upgrades and software downloaded from the internet, must be

submitted to ICT Support. ICT Support will facilitate procuring and/or installing the software with the ICT software manager in accordance with ICT change management policy and procedures.

This policy also applies to acquiring hardware with pre-installed software.

11.2 Commercial governance

Purchasing software must comply with Commissioner's Financial Instructions (CFIs) and the AFP National Guideline on procurement and contracting

Software must only be purchased from reputable, authorised sellers.

11.3 ICT software manager

ICT must appoint a suitably trained member as the ICT software manager to carry out software administration and software asset management functions in respect of ICT systems managed by ICT.

11.4 Business system software manager

The CIO may agree to decentralised (local) acquisition and administration of software assets in respect of a system not managed by ICT. That system owner must designate a suitably qualified person as a business system software manager to administrate and manage the software for that system.

Nomination details of business system software managers must be forwarded to ICT, via ICT Support Centre

11.5 Free software, freeware and shareware

Free software, freeware and shareware are copyrighted software. If the CIO or system owner approves using it, its authors must be paid for that use and the AFP will comply with any accompanying licence terms and conditions.

Acquiring and registering such software must be handled as if it were a commercial software product.

11.6 Registering software

When purchased software is delivered to the AFP it must be forwarded, before installation, to the ICT software manager or to the appropriate Business system software manager of a non-ICT managed system (where applicable). That manager must then:

- conduct an inventory of the software and any accompanying documentation and manuals
- complete and return any registration documentation to the software manufacturer/publisher or reseller (as indicated on registration documentation) as soon as possible after receipt
- record the details of the software in a software register (see below).

Because of appointee mobility and turnover, software should never be registered in the name of an individual user.

11.7 Record keeping - software register

Software registers must be created and used to provide a continuous, comprehensive and current record of all software distribution and use in the AFP. This helps ensure and demonstrate compliance with all licences and agreements.

The ICT software manager must maintain a register of all AFP software acquired by or through ICT.

The system owner of a non-ICT managed system must ensure a software register for that system is maintained by the nominated business system software manager.

11.8 Working/back-up copies

Where permitted by the relevant licence agreement, the ICT software registrar or a business system software manager (where appropriate) may make working/back-up copies of the original media to facilitate more efficient installation, support and maintenance and/or service continuity response and recovery.

The number of copies made must not exceed that allowed by the licence agreement.

11.9 Storage of software and documentation

The following must be kept in a secure storage facility maintained by the ICT software manager or the relevant business system software manager:

- original media
- working/back-up copies of software not in use
- registration and purchasing information
- original software licences.

11.10 Software Audit

In addition to the annual stock take conducted by the National Assets Team, the ICT software manager and business system software managers of non-ICT managed systems should carry out regular audits and checks of:

- software registers
- original copies of the software media
- all working/back-up copies
- registration and licence documentation.

Records of software audits must be maintained by the appropriate software manager(s).

11.11 Obsolete/superseded software

Unless otherwise directed, copies of software no longer licensed for use and/or superseded by new versions must be destroyed or otherwise disposed of according to the relevant licence agreement.

12. Virus checks

All software and magnetic or optical media used to transfer or copy data, including programs and other files downloaded from the internet must be scanned with virus detection software before installing or executing.

All appropriate precautions should be taken to detect viruses and, if necessary, to prevent them spreading.

12.1 Reporting virus infection

Virus discovery must be reported as required by the AFP National Guideline on the Security Incident Reporting Scheme.

13. Removing/deleting software

System users must not remove or delete software from AFP ICT systems.

Removing or deleting software must be done only by:

- authorised ICT staff; or
- persons authorised by a system owner of a system not managed by ICT.

Details of software removal/deletion must be recorded in the appropriate software register or file.

14. Change management

Installing and uninstalling software must comply with change management guidelines and procedures developed and published by ICT.

15. Software use

15.1 Software licence compliance

AFP approved software use must comply with the relevant licence.

Appointees must not use software unless the AFP first obtains the appropriate software licence(s).

15.2 Disposal outside of the AFP

AFP owned or leased software must not to be loaned or otherwise disposed of outside the AFP unless specifically authorised by the appointees Manager or Coordinator.

Disposal must comply with the relevant software licence agreement and Commissioner's Financial Instructions.

15.3 Additional copies of software

Except as detailed in Section 10 of this guideline, AFP owned or leased software must not be copied unless specifically authorised by the appointee's Manager or Coordinator

Authorised additional copies of software must comply with the relevant software licence agreement.

Details of producing and/or issuing copies of software must be entered in the appropriate software register.

16. Internet

Unless otherwise noted, all software, music and audiovisual works found in the Internet shall be considered copyrighted works. Even when material is not marked with the copyright symbol ©, appointees should assume all materials are protected under copyright law. Therefore users of AFP systems are prohibited from downloading these files without explicit permission from the copyright holder.

AFP appointees should not place AFP official material, including copyrighted software, on any publicly accessible Internet computer without prior permission.

17. Misuse, loss or theft

Appointees must report any unlawful or unauthorised software installation, copying, use, distribution or transmission in the AFP as per their obligations under the AFP Commissioner's Order on Professional Standards (CO2) for conduct and practice issues.

Loss or theft of software must be reported per s. 8.2 of the AFP National Guideline on the Security Incident Reporting Scheme. Other suspicious incidents must also be considered as potential 'ICT security incidents' and reported accordingly.

The AFP may hold individual AFP appointees liable for any unlawful software acquisition, duplication or usage in the AFP.

18. Further advice

Questions about software management policy should initially be directed to ICT Support.

19. References

Legislation

- *Australian Federal Police Act 1979* (Cth)
- *Copyright Act 1968* (Cth).

AFP governance instruments

- Commissioner's Financial Instructions
- AFP National Guideline on Information Technology (IT) Security
- AFP National Guideline on home-based work
- AFP National Guideline for occasional work at home - security
- AFP National Guideline on procurement and contracting
- AFP National Guideline on the Security Incident Reporting
- AFP National Guideline on the use of removable data storage devices

Other sources

- Australian Government Protective Security Policy Framework.

20. Attachments

- Attachment 1 – AFP Software Code of Ethics.

Attachment 1: AFP Software Code of Ethics

The unauthorised copying of copyrighted computer software is illegal and is contrary to AFP standards of conduct and business practices.

The AFP does not condone such copying and recognises the following principles as the basis for preventing it within the AFP:

1. We will neither permit nor tolerate the making or use of unauthorised software copies within our organisation under any circumstances.
2. We will provide as soon as practical sufficient quantities of legitimately acquired software to meet all our software needs for computer hardware and operations.
3. We will comply with all licensing terms and conditions regulating the use of any software we acquire.
4. We will enforce strong controls within our organisation to prevent the making or use of unauthorised software copies. These include effective measures to verify compliance with these standards and appropriate disciplinary action for any violation of these standards.
5. We will take steps to inform current and future employees of their legal responsibilities in relation to software theft.