



## Information Policy

<b>Metadata</b>	
<b>Caption</b>	Information Policy
<b>Document Identifier</b>	SP00001
<b>Description</b>	This policy states the principles and strategies for the AFP and its personnel in regards to managing and protecting AFP information and maintaining appropriate security clearances to access the information required for their duties.
<b>Governance Function</b>	ICT Services
<b>Owned by</b>	Chief Information Officer
<b>Date First Approved</b>	1/04/2004 12:00 AM
<b>Contact Person</b>	TL ICT Policy and Governance, Office of the CIO
<b>Date Published</b>	18/02/2007 12:00 AM
<b>Date Modified</b>	5/12/2011
<b>Date Last Reviewed</b>	7/12/2009 12:00 AM
<b>Authorised by</b>	Commissioner
<b>Date of Next Review</b>	7/12/2011 12:00 AM
<b>Review Notification</b>	'GovernanceIS@afp.gov.au'
<b>Instrument Type</b>	Policy
<b>Replaces</b>	SP00001-001
<b>Stakeholders</b>	Project Spectrum, CIO, MSec, Commissioner
<b>Instrument Classification</b>	UNCLASSIFIED

AFP Information is information created, received, used, and maintained regardless of physical form, and information prepared for or produced by the AFP and deemed to be under its control in the conduct of its activities or in pursuance of legal obligations.

Access to reliable information is fundamental to the AFP's provision of effective law enforcement services. There is increasing demand to access AFP information "in the field" both domestically and internationally and also an increasing need for balance between the "need to share" and

the "need to know".

Public confidence in the ability of the Australian Federal Police (AFP) to provide and manage effectively all information, including personal and otherwise sensitive material, requires the application of the highest standards in information management practices, which govern information reliability and security.

To fulfil its obligation to maintain information reliability and security, the AFP requires, promotes and supports the personal integrity of AFP personnel and the integrity of its business processes, information services and information assets. This AFP Information Policy is implemented in the following ways.

AFP Personnel are:

- responsible for managing and protecting AFP information; and
- maintaining appropriate security clearances to access the information required for their duties.

The AFP:

- has an information vision and undertakes regular information planning;
- creates, collects, and maintains information that is relevant, accurate, and complete to meet program, policy, and accountability requirements;
- manages its information as a corporate resource that is: shared without personal ownership, handled in accordance with the security classification restrictions applied to intelligence and other sensitive information; and compliant with relevant Commonwealth legislation, Commonwealth requirements and appropriate standards, including recordkeeping, privacy, security, accessibility and freedom of information;
- protects its information from unauthorised access, disclosure, destruction and from interruptions to availability to ensure continuity of key law enforcement services and business processes;
- fosters a supportive environment for managing and protecting information and provides training to AFP personnel;
- provides access to all non-classified information resources to appropriate AFP personnel;
- holds information in an accessible format so that it can be shared and made available, where appropriate, on a national basis and to meet obligations to other criminal justice agencies and partner organisations;
- has the capability to aggregate comparable AFP data on a national basis;
- optimises the value of information by enabling business processes and systems to share, re-use and reduce duplicate information;
- maximises the quality of information through appropriate processes for creating and collecting new information, and by continually reviewing and correcting existing information;
- optimises the usefulness of information through the use of resource discovery tools, classification tools, and directory management tools;
- implements governance and accountability structures for the management of information;
- considers information management requirements and best practice when designing and acquiring new information services and systems;
- provides viable, reliable and technologically proficient information services;
- has appropriate risk management plans in place for all significant information assets; and
- assesses the effectiveness and efficiency of the management of information throughout its life-cycle.

