

Standards for Victoria Police law enforcement data security

Commissioner for Law Enforcement Data Security

July 2007



Standards for Victoria Police law enforcement data security

Commissioner for Law Enforcement Data Security

July 2007

Acknowledgements

The Commissioner gratefully acknowledges all those who assisted in the preparation of these standards and in particular, the contributions of Andrew Dell, Ros Carter, Matthew Considine, Kim Lajoie, Acting Inspector David Gillard and Acting Inspector Mick Ritchie of the Office of the Commissioner for Law Enforcement Data Security.

Published by
the Commissioner for Law Enforcement Data Security
PO Box 281
World Trade Centre
Melbourne Victoria 8005

July 2007

Also published on:
<http://www.cleds.vic.gov.au>

© Copyright State of Victoria, 2007

This publication is copyright. No part of it may be reproduced by any process except in accordance with the provisions of the Copyright Act 1968.

ISBN 978-0-9803434-3-4

Table of Contents

Foreword	5
Part One – Introduction	7
Part Two – Standards	11
Chapter One – Internal Security Organisation	11
Standard 1	11
Standard 2	12
Chapter Two – Roles and Responsibilities	14
Standard 3	14
Standard 4	16
Standard 5	16
Standard 6	18
Standard 7	20
Chapter Three – Access Control	22
Standard 8	22
Standard 9	24
Standard 10	26
Chapter Four – Release	28
Standard 11	28
Standard 12	30
Standard 13	31
Chapter Five – Physical Security	32
Standard 14	32
Standard 15	35
Standard 16	37
Standard 17	39
Standard 18	40
Standard 19	42
Chapter Six – Remote and Mobile Access	43
Standard 20	43
Standard 21	45
Chapter Seven – Electronic Data Storage Devices	46
Standard 22	46
Chapter Eight – Cryptographic Controls	48
Standard 23	49
Standard 24	51

Table of Contents

Chapter Nine – Law Enforcement Data Systems Acquisition and Development	54
Standard 25	54
Standard 26	57
Chapter Ten – Security Classified Law Enforcement Data	60
Standard 27	62
Standard 28	63
Standard 29	64
Standard 30	65
Chapter Eleven – Risk Management	66
Standard 31	66
Chapter Twelve – Security Incident Management	68
Standard 32	68
Standard 33	71
Chapter Thirteen – Business Continuity Management	72
Standard 34	72
Standard 35	74
Chapter Fourteen – Relationships between Victoria Police and Approved Third Parties	76
Standard 36	76
Standard 37	77
Standard 38	78
Standard 39	79
Chapter Fifteen – Compliance	81
Standard 40	81
Standard 41	82
Standard 42	84
Standard 43	85
Part Three	87
CLEDS functions and powers	87
Definitions	88

Foreword

In the 21st century, more information is able to be collected than ever before, on automated systems that make it easier to find, combine and pass on.

When comprehensive data banks on individuals or investigations are electronically stored and accessed, it doesn't take much for information to get out, whether by system breakdown, carelessness or malice.

Victoria Police has hundreds of electronic and paper data systems and repositories, containing details of millions of people. Personal information is stored on victims of crime and witnesses, as well as those charged and convicted. Anyone involved in an investigation, assisting police, possessing a firearms licence, working as a private investigator or security guard, and all who have applied for criminal records checks, are recorded in police data bases.

There is an undoubted need for Victoria Police to collect, store and use the information required for effective law enforcement.

The community is prepared to trust Victoria Police with a great deal of personal data so that they can do their job properly.

In exchange for that trust, the community has the right to expect that information held by Victoria Police will be secure, used appropriately and disclosed only to those who legitimately need it.

The Standards for Victoria Police Law Enforcement Data Security are established under the *Commissioner for Law Enforcement Data Security Act 2005*. They incorporate the Standards and Protocols for Access to, and Release of, Law Enforcement Data established in March 2007.

Victoria Police is required to adhere to standards so established.

The Chief Commissioner of Police has been consulted on the content of the standards and protocols, which distil for Victoria Police national and international information security standards.

I confidently anticipate the full cooperation of Victoria Police in implementing all necessary measures to assure the security of law enforcement data in accordance with the standards and protocols.

A handwritten signature in black ink, reading "Laurie E Bebbington". The signature is written in a cursive style with a long, sweeping underline that extends to the right.

Laurie Elizabeth Bebbington
Commissioner
Law Enforcement Data Security

July 2007

Part One – Introduction

The *Commissioner for Law Enforcement Data Security Act 2005* ('Act') is intended to *promote the use by the police force of Victoria of appropriate and secure management practices for law enforcement data*.¹ The Act provides for the Commissioner for Law Enforcement Data Security ('CLEDS') to perform several functions, including:

- a) the establishment of appropriate standards for the security and integrity of law enforcement data systems;
- b) the establishment of appropriate standards and protocols for access to, and the release of, law enforcement data, including, but not limited to, the release of law enforcement data to members of the public; and
- c) the conduct of monitoring activities, including audits, to monitor compliance with the standards and protocols established under (a) and (b) above.

Victoria Police must comply with the Standards and Protocols established by the Commissioner for Law Enforcement Data Security.

Law enforcement data is defined broadly in the Act to include all types of data used by Victoria Police for law enforcement purposes. Law enforcement data systems include all relevant data repositories and are not limited to computer systems.

The *Standards for Law Enforcement Data Security* incorporate and replace the *Standards and Protocols for Access to, and Release of, Law Enforcement Data*, published in February 2007, which addressed the specific issue of information access and release².

The Standards outline necessary controls for the secure management of law enforcement data systems and the information they contain. The Standards capture the essence of best practice to be observed in relation to law enforcement data security management.

The Standards represent a distillation for Victoria Police of the national and international benchmark standards on information security. CLEDS acknowledges that the relevant national and international information security benchmarks are:

- a) Organisation for Economic Co-operation and Development *Guidelines on the Protection of Privacy and Transborder Flows of Personal Information*;
- b) *Australian/New Zealand Standard on Information Technology – Security Techniques – Code of Practice for information security management (AS/NZS ISO/IEC 17799:2006)*;
- c) *The Australian Government Protective Security Manual*; and
- d) Defence Signals Directorate *Australian Government Information and Communications Technology Security Manual (ACSI 33)*.

The Commissioner is obliged, under the Act, to consult with the Chief Commissioner of Police when establishing standards and protocols. Such consultation ensures that standards, once promulgated, not only represent best practice in terms of contemporary management of law enforcement data systems security but are also practical, workable and understood by Victoria Police.

In the course of implementing the Standards, Victoria Police will need to develop or amend operating rules and procedures. These Standards build on and strengthen many existing Victoria Police policies and procedures. Existing Victoria Police policies and procedures include:

- a) *Victoria Police Manual (VPM)*;
- b) *Chief Commissioner's Instructions*;

¹ Commissioner for Law Enforcement Data Security Act 2005 – section 1.

² Note that previously published Standards 4 – 20 have been renumbered in this consolidation edition as 3 – 7, 11 – 15, 21, 36 – 40 and 43; previous Standards 1 – 3 are now numbered 8 – 10. Protocols for each of these standards have been similarly renumbered.

Introduction

- c) *Victoria Police Code of Conduct;*
- d) *Victoria Police Enterprise Information Security Policy (September 2004);*
- e) *Law Enforcement Assistance Program Management Unit Standard Operating Procedures;*
- f) *Records Services Division Information Release Policy (21 July 2006);*
- g) *Dealing with Confidential Information (Ethical Standards Division Workbook July 2002);*
- h) *Workplace Inspection Manual (Corporate Management Review Division February 2006).*

This document is divided into three parts. Part 2 contains the 43 standards. The Standards are grouped into fifteen categories:

- a) Internal Security Organisation
- b) Roles and Responsibilities
- c) Access Control
- d) Release
- e) Physical Security
- f) Remote and Mobile Access
- g) Electronic Data Storage Devices
- h) Cryptographic Controls
- i) Acquisition and Development
- j) Classified Law Enforcement Data
- k) Risk Management
- l) Security Incident Management
- m) Business Continuity Management
- n) Relationships between Victoria Police and Approved Third Parties
- o) Compliance.

A definition is provided for each of the major categories, the intended application of the Standard is described, and a statement of objective indicates the purpose of the Standard. Each Standard and Protocol is individually numbered. Where required, guidance is provided to assist Victoria Police when they are implementing the Standards and Protocols. In the areas where the Commissioner is not required under the Act to establish Protocols, more extensive implementation guidance is provided.

Part 3 summarises the functions and powers of CLEDS under the Act, including the ongoing role to monitor and audit Victoria Police compliance with the standards and protocols. Part 3 also provides definitions of terms contained in the document. These are intended to assist in ensuring that the Standards and Protocols are easily understood by those who are required to implement them.

Introduction

Key Definitions

Law Enforcement Data is defined in the Act as any information obtained, received or held by Victoria Police:

- a) for the purpose of one or more of its, or any other law enforcement agency's, law enforcement functions or activities; or
- b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or
- c) in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal; or
- d) for the purposes of its community policing functions.

Such information includes text, images, audio and video held on computing devices or in hard copy format or other storage media, including but not limited to, data relating to individuals or aggregated data, written reports and correspondence, memoranda, police diaries, official notebooks, running sheets and other data repositories.

System generally means a group of elements, components, or devices that are assembled to serve a common purpose. However, in relation to these Standards, system refers to either an information technology system or a non-electronic data repository. In an information technology system, this refers to all hardware, software, networks, cables, peripheral equipment, information, data, personnel, and procedures that comprise a computer environment. While a non-technological system refers to all activities involved in performing particular function/s, a non-electronic data repository refers to repositories such as the Victoria Police official filing system or Sworn Members' police diaries, official notebooks, running sheets and other data repositories.

Access refers to the ability of an individual or organisation to directly retrieve or view law enforcement data or to access a law enforcement data repository. Release means any disclosure of law enforcement data. Release occurs in situations where individuals or organisations are provided with law enforcement data but do not have direct access to the data store. For the purpose of these Standards, the viewing of law enforcement data that has been released in an authorised manner is no longer considered access.

Approved Third Party means an organisation or individual external to Victoria Police that has been granted direct access to Victoria Police law enforcement data repositories.

It is important to note that, for the purposes of this document, law enforcement data to which Approved Third Parties are granted access refers to law enforcement data obtained, received or held by Victoria Police. It does not include other data relating to law enforcement held by the Approved Third Party and that was not obtained from Victoria Police.

Security Classified Information is defined as information that, if compromised, could have adverse consequences. The Security Classification System is an organisation's mechanism for protecting the confidentiality of information generated by it or provided to it. The security classification system is implemented by assigning protective markings, such as TOP SECRET. The protective marking not only shows the value of the information but also indicates the minimum level of protection it must be afforded to safeguard it from compromise.

Victoria Police is often required to handle law enforcement data that requires a security classification to assist in its protection. Victoria Police will assign a classification marking to this information that aligns with Australian Government Security Classifications. The national Security Classification system is described in the *Australian Government Protective Security Manual (PSM)*.

Introduction

Generally all law enforcement data is considered to have a minimum classification of IN-CONFIDENCE, with certain types of sensitive law enforcement data afforded higher Classifications.

Victoria Police accesses, stores and releases certain types of information that is considered national Security Classified information. Typically, this information is generated by, or provided to Victoria Police in relation to its work in counter terrorism or national intelligence activities. For this Australian Government Security Classified information, implementation of the PSM and compliance with its strict controls is mandatory. Chapter 10 *Security Classified Law Enforcement Data* describes Victoria Police's responsibilities in this regard.

Part Two – Standards

Chapter One – Internal Security Organisation

Definition

The term 'internal security organisation' refers to the management structure within Victoria Police that is concerned with the implementation and maintenance of a suitably secure environment for law enforcement data.

Application

These standards apply to Victoria Police.

Standard 1

Victoria Police must implement an information security management structure that is effective in supporting the creation, coordination and maintenance of a secure environment for law enforcement data.

Statement of Objective

To ensure that Victoria Police establishes and maintains an internal information security management framework that is effective in creating and maintaining a secure environment for law enforcement data.

Implementation Guidance

Establishing a management framework is essential to initiate and control the implementation of information security. Such a framework defines a structure which supports Victoria Police to implement effective and coordinated security for law enforcement data.

Documenting a security framework assists users and management to quickly and easily identify where and with whom (usually on a position-basis) all Victoria Police responsibilities reside in relation to the security of law enforcement data.

Effective implementation of information security requires demonstrated management support. Visible and active support for security across the organisation can be achieved through demonstrated commitment, clear direction, and the assignment and acknowledgment of information security responsibilities. In particular management should:

- a) provide clear direction and visible support for security initiatives, identify information security goals, and tailor these to meet Victoria Police requirements;
- b) ensure information security policy is developed, reviewed, and approved;
- c) ensure availability of resources needed for information security;
- d) assign specific roles and responsibilities for information security across Victoria Police;
- e) initiate plans and programs to maintain information security awareness; and
- f) ensure that the implementation of information security controls is co-ordinated across Victoria Police.

The implementation of information security is not solely the responsibility of users and security staff but requires the collaboration of management, administration staff, developers and specialist staff (including auditors, insurance, legal, human resource, education and security personnel).

Internal Security Organisation

The coordination of information security involves:

- a) developing and approving methodologies and processes for reviewing information security, such as:
 - assessing the adequacy and co-ordinating the implementation of information security controls; and
 - risk assessment to identify significant threat changes and exposure of information and information processing facilities to threats;
- b) ensuring that security activities are executed in compliance with an information security policy and a mechanism to respond to non-compliances exists;
- c) evaluating information received from monitoring and reviewing of information security incidents and recommending appropriate actions in response to identified information security incidents; and
- d) effectively promoting information security education, training and awareness throughout the organisation.

In a diverse and decentralised organisation such as Victoria Police, it is very important to establish a single point of coordination regarding security of law enforcement data and security more generally. Whilst not necessarily ultimately responsible for security, a single point of coordination will assist in ensuring a holistic and integrated approach.

Standard 2

Victoria Police must appoint a Security Executive. For handling Australian Government Security Classified law enforcement data, an Agency Security Advisor and an Information Technology Security Advisor should be appointed in accordance with Australian Government protective security standards.

Statement of Objective

Clear, high level organisational responsibility is designated for the security of law enforcement data. In order to meet its responsibilities under the Protective Security Manual for Australian government security classified information (and therefore classified law enforcement data) Victoria Police must also appoint an Agency Security Advisor and an Information Technology Security Advisor.

Implementation Guidance

It is essential that Victoria Police designates a senior executive to have overall responsibility for the security of law enforcement data. Given that Victoria Police law enforcement data includes Australian Government classified information, an Agency Security Advisor (ASA) and Information Technology Security Advisor (ITSA) are also required under the *Australian Government Protective Security Manual*. These two positions may be designated as responsible for the security of all law enforcement data or just nationally classified data.

The Security Executive is a member of the executive management group designated as responsible for the ongoing development of Victoria Police's security policy and the oversight of all matters relating to information security, including law enforcement data. The Security Executive is responsible for providing high-level guidance to the ASA and the ITSA and should also report to the

Internal Security Organisation

Chief Commissioner of Police on information security procedures, incidents and matters of interest or concern.

The role of the Agency Security Advisor is to manage and coordinate Victoria Police's information security functions on a day-to-day basis.

The role of the Information Technology Security Advisor is to oversee Information Communications Technology (ICT) security within Victoria Police, including overseeing the security of information that is stored electronically or otherwise dealt with using Victoria Police's ICT systems.

Both the ASA and the ITSA should report to the Security Executive who should, in turn, report to the Chief Commissioner of Police

In addition to possessing general information security qualifications, knowledge and experience commensurate with the role, both the ASA and the ITSA must be trained in Australian Government and Victoria Police protective security policy, principles and minimum standards. Both positions should be sufficiently senior to enable the respective office holders to effectively develop and implement protective security arrangements for Victoria Police in conjunction with senior management.

Chapter Two – Roles and Responsibilities

Definition

Victoria Police must ensure that all Victoria Police employees understand their roles and responsibilities in relation to information security.

When engaging a contractor or consultant, Victoria Police remains accountable for the secure performance of the function that the contractor or consultant is to perform. Victoria Police must ensure that contractors and consultants are fully aware of the information security policies and guidelines and that they undertake appropriate security precautions when handling law enforcement data and performing functions for Victoria Police.

Victoria Police must require that all Approved Third Parties have information security policies and procedures that reflect Victoria Police law enforcement data security requirements. Approved Third Parties must also be required to ensure that all staff who access law enforcement data are fully aware of the information security policies and guidelines and that they undertake appropriate security precautions when handling law enforcement data.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 3

The security roles and responsibilities of Victoria Police Employees, Contractors, Consultants and Approved Third Parties in relation to the secure management of law enforcement data must be defined and documented in Victoria Police's Information Security Policy.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to define and document in an Information Security Policy, the roles and responsibilities in relation to the secure management of law enforcement data.

Statement of Objective

The definition and documentation of security roles and responsibilities in the Victoria Police Information Security Policy should aim to provide clear guidance and a common understanding of these roles and responsibilities to all Victoria Police employees, contractors, consultants and Approved Third Parties. It will also provide the basis for training on the roles and responsibilities and for measuring compliance.

Roles and Responsibilities

Protocol 3.1

Victoria Police's Information Security Policy must be approved by the Chief Commissioner of Police, be published and communicated to all Victoria Police employees, contractors, consultants and Approved Third Parties and contain statements relevant to access to, and release of law enforcement data including:

- a) a definition of general and specific responsibilities for the secure management of law enforcement data including reporting information security incidents;
- b) a statement of management intent, supporting the goals and principles of law enforcement data security in line with Victoria Police business strategy and objectives;
- c) a brief explanation of the security policies, principles, standards and compliance requirements of particular importance to Victoria Police, including:
 - compliance with any relevant legal requirements, including legislative, regulatory and contractual requirements;
 - information security education, training and awareness requirements; and
 - the consequences of information security breaches.

Information security roles and responsibilities must include the requirement to:

- a) implement and act in accordance with Victoria Police's information security policies;
- b) protect assets from unauthorised access, release, modification, destruction or interference; and
- c) ensure responsibility is assigned to the individual for actions taken by that individual.

The Information Security Policy must be communicated throughout Victoria Police to all who access law enforcement data in a form and manner that is relevant, accessible and understandable to the intended reader.

The Information Security Policy must be reviewed at regular planned intervals or when significant changes occur, to ensure its continuing suitability, adequacy and effectiveness.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement for the development of an Information Security Policy which specifies adherence to the requirements detailed in Protocol 3.1, as they would apply to the Approved Third Party.

Implementation Guidance

Further advice on the process for reviewing an information security policy is available in Section 5.1.2 of the AS/NZS 17799, Code of Practice for Information Security Management, 2006.

Roles and Responsibilities

Standard 4

Information security responsibilities must be addressed prior to initial employment in job descriptions and documentation prepared for the engagement of Employees, Consultants and Contractors.

Statement of Objective

The inclusion of information security responsibilities in job descriptions and documentation prepared for positions within Victoria Police and in relation to the engagement of consultants and contractors, aims to provide prospective and new Victoria Police employees, contractors and consultants with an understanding of their law enforcement data security responsibilities prior to commencing employment.

Protocol 4.1

Job descriptions and documentation prepared for the engagement of employees, consultants and contractors must include reference to Victoria Police's information security policy and briefly outline the information security principles, standards and compliance requirements of particular importance to Victoria Police.

All position advertisements and background documentation prepared for employees, contractors and consultants must contain a reference to the appointment being dependent upon a full security check, including fingerprinting.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that information security responsibilities be addressed in job descriptions or in relevant background documentation provided for positions that will require access to law enforcement data.

Standard 5

Victoria Police Employees, Contractors, Consultants and Approved Third Parties must sign an agreement on their security roles and responsibilities, including a confidentiality agreement.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that users sign an agreement on their law enforcement data security roles and responsibilities, including a confidentiality agreement.

Statement of Objective

Implementation of this standard will assure Victoria Police that those who access law enforcement data have read and agreed to comply with the relevant policies, plans and procedures for the systems they are using.

Roles and Responsibilities

Protocol 5.1

Victoria Police must ensure that Victoria Police employees, contractors, consultants and Approved Third Parties agree to terms and conditions concerning information security appropriate to the nature and extent of access they will have to the organisation's law enforcement data assets.

The terms and conditions of the Agreement must reflect Victoria Police's information security policies and provide details of the following responsibilities:

- a) the legal responsibilities and rights of Victoria Police employees, contractors, consultants and Approved Third Parties regarding copyright laws or data protection legislation;
- b) responsibilities for the classification of information and management of Victoria Police law enforcement data assets handled by the individual or entity concerned;
- c) responsibilities of the Victoria Police employee, contractor, consultant or Approved Third Party user for the handling of information received from other organisations;
- d) Victoria Police's responsibilities in relation to the handling of personal information, including personal information created as a result of, or in the course of, employment with Victoria Police;
- e) responsibilities that are extended beyond Victoria Police's physical premises and outside normal working hours, such as in the case of working from home; and
- f) actions to be taken if the Victoria Police employee, contractor, consultant or Approved Third Party user disregards Victoria Police's information security requirements.

Where appropriate, information security responsibilities contained within the Agreement should continue for a defined period after the end of the employment.

The terms and conditions of employment or engagement must require that all Victoria Police employees, contractors, consultants and Approved Third Parties who are given access to law enforcement data must sign a confidentiality or non-disclosure agreement prior to being given access to the data.

Implementation Guidance

In addition to the protocols above, Codes of Conduct of Victoria Police and the State Public Service may also be used to address the responsibilities of Victoria Police employees and contractors, regarding confidentiality, data protection, ethics, appropriate use of Victoria Police's assets and facilities, as well as reputable practices expected by Victoria Police.

Roles and Responsibilities

Standard 6

A formal disciplinary process must be established for Victoria Police Employees, Contractors and Consultants, who are considered to have been involved in a breach of law enforcement data security.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to establish a formal disciplinary process for users who are considered to have been involved in a breach of law enforcement data security.

Statement of Objective

The establishment and implementation of formal disciplinary procedures for Victoria Police employees, contractors and consultants who are considered to have committed a security breach aims to maintain established Victoria Police standards of behaviour and complies with legislative requirements.

Protocol 6.1

Unless specifically authorised by law or direction from their supervisor, Victoria Police employees, contractors and consultants must not access or release any law enforcement data other than is legitimately required to discharge their duties.

Known or suspected misuse of law enforcement data, including the following incident types, must be reported:

- a) attempts to access law enforcement data by unauthorised users;
- b) attempts to access law enforcement data for an unauthorised purpose by an authorised user; and
- c) unauthorised use of law enforcement data by any users that could be categorised as instances of corruption, criminality or serious misconduct.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to report details of the following to Victoria Police:

- a) attempts to access law enforcement data by unauthorised users;
- b) attempts to access law enforcement data for an unauthorised purpose by an authorised user; and
- c) unauthorised use of law enforcement data by any users that could be categorised as instances of corruption, criminality or serious misconduct.

Implementation Guidance

Victoria Police employees, contractors and consultants are granted authorised access to law enforcement data to help them undertake their day-to-day duties. Such access is a privilege and those with access rights should be aware that apart from legitimate business-related purposes, there is no instance where a Victoria Police user should have access to law enforcement data relating to members of the community that is over and above that of any other citizen.

Roles and Responsibilities

The misuse of law enforcement data and privileges relevant to access and release may include, but is not restricted to, the following:

- a) accessing or releasing any law enforcement data (or information accessible to the user as a representative of Victoria Police) for which the user does not have an authorised Victoria Police business need;
- b) attempting to use previously authorised access privileges following termination of employment or contract with Victoria Police, irrespective of whether or not those access privileges have been revoked or removed;
- c) attempting to modify or remove law enforcement data without proper authorisation;
- d) attempting to use, or using, any other person's User ID;
- e) attempting to test, bypass or defeat any security safeguards established to protect law enforcement data without proper authorisation;
- f) circumventing or attempting to circumvent assigned access limits, logon procedures or assigned privileges;
- g) sending fraudulent electronic mail, breaking into another user's mailbox or reading their electronic mail without permission;
- h) sending any fraudulent electronic transmission;
- i) introducing or using unauthorised, untested, unlicensed (by Victoria Police) or illegal software that may introduce unknown and/or malicious security vulnerabilities;
- j) harassing or threatening other users or interfering with their access to law enforcement data;
- k) taking advantage of another user's naivety or negligence to gain access to law enforcement data for which they have not been authorised; and
- l) disclosing or removing third party proprietary information.

A careless or accidental breach may involve disciplinary or remedial action, including counselling, training or both, while deliberate breaches should be classified as corruption, serious or minor misconduct or a breach of discipline and may result in disciplinary or criminal sanctions.

Victoria Police has established discipline processes and procedures managed by the Ethical Standard Department. Details of the discipline processes and procedures are provided in the Victoria Police Manual.

Roles and Responsibilities

Standard 7

All Victoria Police Employees, Contractors and Consultants must receive appropriate induction and ongoing information security awareness training as relevant for their job functions.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement for all law enforcement data users to receive appropriate induction and ongoing information security awareness training as relevant for their job functions.

Statement of Objective

The provision of induction and ongoing information security awareness training to Victoria Police employees, contractors, consultants and Approved Third Parties is intended to ensure that authorised users of law enforcement data understand their information security roles and responsibilities.

Protocol 7.1

Victoria Police must ensure that information security awareness training is provided for all Victoria Police employees who use or provide services in support of law enforcement data.

Victoria Police must require that any Approved Third Parties provide all training necessary to safeguard the security of law enforcement data that is accessed, managed, developed or implemented by them to all relevant staff.

The Information Security Awareness Training must:

- a) provide awareness of the Victoria Police Information Security Policy for all existing and new users of Victoria Police law enforcement data;
- b) address general responsibilities and basic information security procedures affecting all persons who use, or provide services in support of, law enforcement data;
- c) provide individual staff with documentation of, and training in, key operating procedures for security-related tasks relevant to their position and/or responsibilities;
- d) provide awareness of the Victoria Police auditing capability and its aims to proactively detect the misuse of law enforcement data;
- e) include identification, reporting and response procedures for information security incidents; and
- f) be updated as the Victoria Police Information Security policies, standards, guidelines, procedures and System Security Plans are revised.

Victoria Police sworn members must be provided with information security awareness training as part of their recruit training and upon promotion to the rank of Sergeant and Inspector.

Roles and Responsibilities

Implementation Guidance

It is the responsibility of managers at all levels to ensure that knowledge of, and training in, the information security safeguards implemented to protect law enforcement data is provided for all users of that data.

Individual workplaces (in particular, those that regularly create, access, use or release security classified information) must ensure that employees are instructed on Victoria Police's expectations and their personal responsibilities regarding the handling of security classified information.

Chapter Three – Access Control

Definition

Access Control refers to a service or technique used to permit or deny access to law enforcement data, or law enforcement data repositories. It is used to define or restrict the rights of individuals or information systems to access and use data.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 8

Victoria Police Employees, Contractors, Consultants and Approved Third Parties must be deemed suitable prior to being granted access to law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties who access law enforcement data require all users to undergo a security check.

Statement of Objective

The requirement for all Victoria Police employees, contractors and consultants and Approved Third Party users to undergo a background check prior to being granted access to law enforcement data is intended to ensure that only those individuals and entities that are suitable and eligible are granted access to law enforcement data.

Access Control

Protocol 8.1

The judgement of suitability to access law enforcement data will include satisfying the requirements of a full security check.

A full security check must comprise at a minimum:

- a) a name search of the National Names Index, however titled;
- b) a name search of LEAP and/or other jurisdictions where identified by the search of the National Names Index;
- c) a search of LEAP for pending charges; and
- d) a comparison of the prospective user's fingerprints with those kept on the National Automated Fingerprint Identification System (NAFIS) register, however titled.

A full security check will include details of all court convictions, guilty verdicts or custodial sentences. Details of all outstanding charges or pending matters will also be included.

Based on information revealed by the full security check, access must be denied if the check reveals that the prospective user may constitute an unacceptable security risk or is deemed unsuitable for any other reason.

In addition to a full security check, measures must be taken to ensure that a person requesting access has not for any reason been denied access to law enforcement data or had their access rights revoked in the past. If a check reveals that access has previously been denied or revoked, the suitability of the applicant must be reviewed.

Measures should be established to periodically review security checks to ensure continued suitability to access law enforcement data.

Implementation Guidance

Security screening seeks to establish that existing or prospective employees, contractors or consultants:

- a) are eligible to have access;
- b) have had their identity established; and
- c) are suitable to have access.

Victoria Police has detailed instructions and protocols that cover all security and background checks in the Victoria Police Manual.

All sworn members are subject to full security checks associated with their induction.

Public Servants, Contractors and Consultants employed by Victoria Police who require access to and/or use of Victoria Police facilities, and therefore have the potential to access law enforcement data in the course of their duties must undergo a full security check prior to commencing duties with Victoria Police. This includes the recommended applicant for every public servant position, including on-going, fixed term and casual positions.

No Victoria Police employee, contractor or consultant may receive access to law enforcement data until deemed suitable via a full security check and the result has been documented. In implementation, it should be noted that even if a person is deemed suitable by the initial full security check, circumstances and suitability may change, hence mechanisms to review and maintain suitability should be developed.

Victoria Police employees, contractors or consultants who require access to Australian Government security classified information require further security checks in order to gain a security clearance. Standard 29 outlines the requirements of this process.

Access Control

Standard 9

An access control policy must be established, documented and reviewed based on business and security requirements for access to law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to maintain an access control policy.

Statement of Objective

Access control rules and rights for each user or group of users should be clearly stated in an access control policy. The policy aims to ensure authorised user access and to prevent unauthorised access to law enforcement data.

Access control policies aid in preventing unauthorised user access, and compromise or theft of law enforcement data. The co-operation of authorised users is essential for effective security. Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of computing devices.

Protocol 9.1

The access control policy must:

- a) require formal authorisation and periodic review, and describe a revocation process for access rights;
- b) address authorisation for access to law enforcement data, including “need to know” and be consistent with information classification policies;
- c) describe standard user access profiles for common access requirements based on job roles;
- d) recognise and address access rights and types for all types of connections (both internal and external) available in a networked environment;
- e) identify all law enforcement data stored or processed by the system and the associated security risks;
- f) address relevant legal obligations, including compliance with relevant legislation, contractual obligations and memoranda of understanding regarding protection of access to law enforcement data; and
- g) ensure segregation of responsibilities for controlling access. For example, access request, access authorisation and access administration.

Access Control

Protocol 9.2

There must be a formal user registration and de-registration procedure in place for granting and revoking access to all electronic law enforcement data. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require or are no longer authorised to have access to law enforcement data.

Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls. Regular user activities must not be performed from privileged accounts.

Access control procedures for user registration and de-registration must include requirements for:

- a) assigning unique user IDs to enable users to be audited and held responsible for their actions. Shared or group IDs must not issued;
- b) ensuring that the user has authorisation from the system owner;
- c) ensuring that the level of access granted is consistent with Victoria Police security policy;
- d) users to be provided with a written statement of their access rights and that users sign statements indicating that they understand the conditions of access;
- e) maintaining a current auditable record of all registered users, including active, suspended and disabled accounts;
- f) immediately reviewing and if appropriate, removing or blocking the access rights of users who have changed roles or jobs; are no longer Victoria Police employees, contractors or consultants; no longer require access; or are not authorised to have access, for whatever reason; and
- g) scheduling periodical identification of unused or unneeded user accounts (and disabling where appropriate).

Protocol 9.3

Access to law enforcement data must be no wider than is required for the efficient conduct of Victoria Police business and must be restricted to those who are authorised to have access.

This control must be applied for all types of users (including technical support personnel, general Victoria Police and Approved Third Party users, network administrators, system programmers, and database administrators).

Protocol 9.4

Each user account must be allocated a unique ID for individual use only. A suitable authentication method must verify that each account is being used by the correct person.

This requirement is applicable to all types of users including database administrators, system programmers, network administrators, operators and technical support personnel.

The unique IDs are to be used to trace user activities to the responsible individual.

Access Control

Protocol 9.5

The allocation of passwords must be controlled through a formal management process.

Users must be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.

The process must include the following requirements:

- a) users must be required to sign a statement to keep personal passwords confidential;
- b) when users are required to maintain their own passwords they must be provided initially with a secure temporary password, which they must change immediately;
- c) procedures must be established to verify the identity of a user prior to providing a new, replacement or temporary password;
- d) temporary passwords must be issued to users in a secure manner. Conveying the password through an unauthorised third party or unprotected (clear text) electronic mail messages must not occur;
- e) temporary passwords must be unique to an individual and must not be guessable;
- f) users must acknowledge receipt of passwords;
- g) passwords must never be stored in an unprotected form;
- h) default vendor passwords must be altered following installation of systems or software; and
- i) Specific password controls include:
 - passwords to be changed at least every 90 days;
 - users to be prevented from changing their password more than once a day;
 - passwords to be checked for poor choices; and
 - users to be forced to change an expired password on initial logon or if reset.

Standard 10

Procedures for monitoring access to law enforcement data must be established and the results of the monitoring activities reviewed regularly.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement for monitoring access activities to law enforcement data.

Statement of Objective

This standard aims to detect access control events and to trace users to their activities. Logging must be used to verify compliance with the access control policy.

Access Control

Protocol 10.1

To effectively capture information relevant to access and release of law enforcement data, the following activities must be logged:

- a) successful authorised activities, including:
 - the user and terminal ID;
 - the date and time of access events (such as login, logout, and file access);
 - the types of events;
 - the applications accessed; and
 - the files and information accessed;
- b) privileged user and administrative activities including:
 - use of privileged accounts;
 - process manipulation; and
 - system start-up and shut down;
- c) unauthorised access attempts, including:
 - failed or rejected logon or file access attempts;
 - failed or rejected actions involving law enforcement data;
 - access control policy violations; and
 - notifications and alerts for network gateways, firewalls and intrusion detection systems;
- d) system alerts or failures including:
 - attempts to change system settings (whether successful or unsuccessful);
 - access control systems alarms;
 - network management alarms;
 - system log exceptions; and
 - console alerts or messages.

All logs must be stored and kept for a sufficient period of time to allow audit activities, such as detection, tracing, and verification of access.

An independent internal Victoria Police audit facility must be established with access to logging information. Such audit must proactively examine log information to identify any possible misuse of law enforcement data.

Implementation Guidance

Authoritative guidance on system logging is found at AS/NZS ISO/IEC 17799:2006 (section 10.10.2) and is replicated as Protocol 10.1.

Logging information can also be used to assist users to identify inappropriate use of their access privileges. Victoria Police should consider building certain aspects of logged information into software applications to present users with information such as 'Last Logged In Time and Date' upon initial system access. This information might alert the user to unauthorised use or access attempts that should then be reported.

Chapter Four – Release

Definition

Release refers to any disclosure of law enforcement data.

Authorised Release means release that is sanctioned by law and Victoria Police policy.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 11

Release of law enforcement data must only occur if that disclosure is authorised.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that release of law enforcement data must only occur if it is authorised.

Statement of Objective

This standard aims to prevent the unauthorised release of law enforcement data by requiring that procedures are established that ensure that all disclosure is controlled and the recipients are informed of their responsibilities.

Protocol 11.1

Users must not release any information except where the release or communication of that information is authorised by:

- a) Law; and/or
- b) Victoria Police policy.

Protocol 11.2

Victoria Police must develop and promulgate policy and operating procedures in relation to the release of law enforcement data that, at a minimum, address the following:

- a) the types of release that exist within Victoria Police, including law enforcement data released to:
 - other employees, contractors or consultants;
 - members of the public;
 - the media/press; and
 - other third parties;
- b) that the release of law enforcement data occurs in many forms including:
 - verbally;
 - in written form or printed text;
 - via multimedia, such as images, video, audio; and
 - via computing systems and devices;
- c) what constitutes unauthorised release;
- d) the process for approving and authorising all release;
- e) roles and responsibilities for all forms of release; and
- f) the requirement to record and maintain a formal record of receipt for law enforcement data released (for law enforcement data released via computing systems, electronic log files suffice).

Protocol 11.3

Victoria Police must develop and promulgate policy and operating procedures, and establish mechanisms to regularly monitor and audit the release of law enforcement data. The results of this monitoring must capture, where appropriate:

- a) what data was released;
- b) to whom it was released;
- c) who authorised the release;
- d) who released the data; and
- e) where, when and how the data was released.

Protocol 11.4

Victoria Police must develop, publish and regularly review information bulletins describing scenarios and case studies which highlight appropriate release and discourage inappropriate release of law enforcement data. Such guidance should serve all employees, contractors and consultants:

- a) by reminding them of their roles and responsibilities;
- b) by providing quick and effective advice and reference material; and
- c) by providing strategies for minimising accidental release.

Release

Protocol 11.5

When releasing law enforcement data to members of the public or third parties not covered by an Agreement, Victoria Police must apply strict controls and processes to ensure that the release is authorised and that the recipient is fully aware of their responsibilities.

Implementation Guidance

Victoria Police has detailed instructions and protocols that cover the release of law enforcement data. Detailed instructions can be found in the Victoria Police Manual at:

208 – 1 Release of Information – general principles

208 – 2 Release of Information to the media

208 – 3 Release and use of LEAP and related information

208 – 4 Release and use of police records and criminal histories

208 – 5 Release and use of accident and property records

208 – 6 Release of statistical information

208 – 7 Releasing information for court proceedings, inquiries and investigations

208 – 8 Release of Victoria Police personal records

208 – 9 Releasing and advising on Victoria Police policies and publications

Standard 12

Law enforcement data passed to members of the public and other third parties via electronic messaging (including email) must be appropriately protected.

Statement of Objective

Electronic messaging such as email and instant messaging play an increasingly important role in communications. This standard aims to prevent unauthorised release of law enforcement data through the use of electronic messaging.

Protocol 12.1

Security controls for electronic messaging must ensure that:

- a) messages are formatted to provide correct addressing and delivery;
- b) protection mechanisms, such as encryption, adequately protect the contents of the message from access or modification by anyone other than the intended recipient;
- c) the system is reliable and available;
- d) all messages are audited; and
- e) services such as file sharing or instant messaging are strongly discouraged. If used, such services must be tested to ensure no compromise of system security and user access be approved on an individual basis.

Standard 13

Disposal of law enforcement data must be authorised and occur in a timely fashion.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that the disposal of law enforcement data be authorised and occur in a timely fashion.

Statement of Objective

By ensuring that the disposal of law enforcement data is authorised and occurs in a timely manner, Victoria Police can significantly reduce the threat of unauthorised disclosure.

Protocol 13.1

Disposal must be performed:

- a) in accordance with legal and archive requirements;
- b) as quickly as practicable, particularly security classified material that is out of date;
and
- c) with care, to avoid inappropriate disclosure of law enforcement data.

Hard copy law enforcement data must be stored in waste containers, pending destruction, that meet the security requirements appropriate to the security classification of that data.

The deletion of electronic law enforcement data from data storage devices must occur in accordance with government standards (appropriate to the security classification).

The disposal of all data storage devices that have previously contained law enforcement data is to occur such that no law enforcement data can be recovered.

When law enforcement data is moved prior to destruction, the manner and method of carriage must comply with security safeguards relating to the security classification of the data.

Implementation Guidance

Further advice is provided in the Victoria Police Manual including:

- 206 – 2 Document Security
- 209 – 1 Archiving Information
- 209 – 2 Records Disposal

Chapter Five – Physical Security

Definition

Physical security is the application of material measures designed to protect law enforcement data from unauthorised access, destruction, use, modification or release.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 14

Victoria Police must ensure that all facilities that access, store or handle law enforcement data are physically protected against unauthorised access.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to ensure that all facilities that access, store or handle law enforcement data are physically protected against unauthorised access.

Statement of Objective

To prevent unauthorised access to law enforcement data by the creation of a secure physical environment.

Protocol 14.1

An assessment of the security risk must occur for every Victoria Police facility to determine the exact nature of the physical security measures appropriate for that facility, having regard to the objective of preventing unauthorised access to law enforcement data.

An assessment of the security risk must be carried out in each of the following circumstances:

- a) for any existing or new site where law enforcement data is, or is to be, stored, processed or handled;
- b) whenever a significant change occurs to the assessed threat to an existing site; and
- c) whenever a change, either addition or loss, of a significant function occurs at a Victoria Police premises.

The assessment of the security risk must be specific to particular facilities and should address all relevant matters, including:

- a) the location and nature of the facility;
- b) whether Victoria Police has sole or shared ownership or tenancy of the facility;
- c) whether the public or other non-Victoria Police personnel have a right to enter the site on which the facility is located;
- d) the nature of the law enforcement data contained on, or processed by, the facility;

Standards and Protocols

Physical Security

- e) the nature and location of supporting utilities, such as electricity, water, sewage, heating/ventilation and air conditioning and, in particular, whether these facilities are adequate for the systems they are supporting;
- f) whether any protective measures are required to prevent accidental or malicious damage to power and telecommunications cabling carrying law enforcement data or supporting the carriage of law enforcement data to or from the facility and, if so, the nature of the protective measures; and
- g) whether the facility is vulnerable to any environmental risks or other external occurrences, including an attack by terrorists, which might pose a threat to the security of law enforcement data.

Protocol 14.2

Clearly defined Security perimeters must be employed to protect areas in which Victoria Police facilities are located. The following matters must be addressed, as appropriate, in relation to the establishment of physical security perimeters and the creation of secure areas for the location of facilities:

- a) the strength and siting of each perimeter must be determined by the protection requirements of the law enforcement data contained or processed within the perimeter, as determined by the security risk assessment for that facility;
- b) buildings or facilities containing law enforcement data must be physically protected against intrusion by accidental or unlawful means. In particular, the external walls of the perimeter must be of solid construction and all external doors and windows must be suitably protected against unauthorised access with appropriate control mechanisms, such as locks, bars, alarms, security lighting and closed circuit television;
- c) facilities must, if possible, be physically separated from other facilities managed or operated by third parties; and
- d) a staffed reception area or other means to control physical access to the secure area must be established to ensure that access is limited to authorised personnel. Appropriate entry controls may include:
 - a formal process for the security clearance of all employees in accordance with the access control policy;
 - the implementation of an electronic access control system;
 - a formal process for the authorisation of access by contractors, consultants and other third parties for specific, authorised purposes only;
 - a procedure for recording the date and time of entry and departure by all visitors, (which term includes contractors and third party users/support personnel), during both operational and non-operational hours;
 - a procedure for access rights to secure areas to be regularly reviewed to ensure that they are consistent with the access control policy; and
 - the installation of suitable intruder detection systems covering all external doors and windows. These must be regularly tested.

Physical Security

Protocol 14.3

Appropriate physical security controls must be applied to Victoria Police external access points such as delivery and loading areas to prevent any unauthorised access to law enforcement data. If possible, these areas must be isolated from any secure areas where facilities are located.

Arrangements must include:

- a) appropriate controls on access to external access points;
- b) the design of these areas to ensure that deliveries can occur without unauthorised personnel gaining physical access to any secure area;
- c) the inspection of all incoming material before its removal from the delivery area to the point of use;
- d) a procedure for the registration of all incoming material in accordance with appropriate asset management procedures; and
- e) the physical separation, where possible, of all incoming and outgoing shipments of material.

Protocol 14.4

Victoria Police must develop and implement an appropriate training and education program to ensure that all employees are aware of their roles and responsibilities in relation to physical security measures designed to protect law enforcement data.

Protocol 14.5

Victoria Police must ensure that Agreements with Approved Third Parties require that they assess risk and apply security controls to ensure that facilities that access, store or handle law enforcement data are physically protected against unauthorised access.

Implementation Guidance

An assessment of the security risk can be performed in various levels of detail, ranging from a formal documented Risk Assessment conducted by an external professional security consultancy to an informal undocumented assessment conducted by an individual user on an 'as required' basis.

The decision as to the level of formality of the assessment should be based on the type of law enforcement data and the location involved. An isolated Victoria Police premises that stores large amounts of extremely sensitive law enforcement data (the compromise of which would have severe consequences) would require a formal, documented Risk Assessment. An individual who is working from home on a task that involves non-Security Classified law enforcement data might only need to conduct a mental appreciation of any factors that could compromise security and implement adequate countermeasures or controls to reduce the risk.

Regardless of the formality of the assessment, Victoria Police should ensure that individuals who work with law enforcement data have an effective working knowledge of risk assessments, are provided with the requisite tools and are able to demonstrate their awareness and understanding of their responsibilities.

More detailed guidance on risk assessment is provided in *Chapter Eleven – Risk Management*.

Standard 15

Appropriate physical security measures must be implemented to protect law enforcement data stored in portable computing and data storage devices or during physical transport outside of Victoria Police premises.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to apply appropriate security measures in respect of the carriage, use and storage of law enforcement data, portable computing devices or portable data storage devices that contain law enforcement data.

Statement of Objective

Law enforcement data stored on portable devices or in physical transit outside Victoria Police premises is potentially more vulnerable to unauthorised access. This standard identifies strategies that will assist in reducing the threat of a security breach.

Protocol 15.1

Business rules for protecting law enforcement data held on portable computing devices and data storage devices must include the following:

- a) portable computing devices and data storage devices must, where possible, be carried as hand luggage and appear inconspicuous when in transit;
- b) portable computing devices and data storage devices must be physically protected against theft, must not be left unattended in a public place and, where possible, must be physically locked away when not in use;
- c) manufacturers' instructions regarding the proper use, maintenance and protection of the equipment must be observed at all times;
- d) where Victoria Police employees work outside Victoria Police premises, appropriate controls to ensure the creation and maintenance of suitable security must be implemented, as determined by an assessment of the security risk for the specific location with regard for the type of law enforcement data; and
- e) procedures to ensure that mobile terminals in vehicles are secured when the vehicle is not occupied by an authorised user.

Implementation Guidance

An assessment of the security risk can be performed with various levels of detail. The decision as to the level of formality of the assessment should be based on the type of law enforcement data and the location involved. An informal assessment may suffice in many cases where a Victoria Police employee works from a location outside Victoria Police premises.

Physical Security

Protocol 15.2

Law enforcement data can be vulnerable to unauthorised access, misuse or corruption during physical transport, for instance when sending law enforcement data via the postal service or via courier. Arrangements to protect law enforcement data being transported between sites, including to and from third parties, must include the following:

- a) reliable transport or couriers must be used;
- b) a list of authorised couriers must be established;
- c) procedures to check the identification of couriers must be developed;
- d) packaging must be sufficient to protect the contents from any physical damage likely to arise during transit and in accordance with any manufacturers' specifications. For example, protecting against any environmental factors that may reduce the ability to retrieve the law enforcement data, such as exposure to heat, moisture or electromagnetic fields;
- e) controls must be adopted, where necessary, to protect law enforcement data from unauthorised disclosure or modification, such as:
 - the use of locked containers;
 - delivery by hand; and
 - the use of tamper-evident packaging (which reveals any attempt to gain access); and
- f) in exceptional cases, splitting of the consignment into more than one delivery and dispatch by different routes.

Standard 16

All Victoria Police facilities that access, store or handle law enforcement data must have physical security controls that reduce the risk of disruptions to service caused by external or environmental threats and safeguard the provision of supporting infrastructure services.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to ensure that all facilities that access, store or handle law enforcement data have physical security controls that reduce the risk of disruptions to service caused by external or environmental threats and safeguard the provision of supporting infrastructure services.

Statement of Objective

To protect supporting services on which the maintenance of a secure infrastructure for law enforcement data relies. Law enforcement data systems and their security systems rely on supporting services, such as connections to the electricity and water supply to function effectively and ensure continued operation during a disaster or crisis.

Implementation Guidance

Protecting the provision of supporting services on which law enforcement data system security relies is essential to the maintenance of a secure environment and aims to minimise the impact of unpredicted events such as natural disasters, or a fire/explosion in a nearby facility. Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

Security systems such as alarms, disaster recovery, and computer auditing services are often sensitive systems that rely upon controlled environments, regulated for temperature and moisture, to perform effectively.

Supporting infrastructure services include electricity, water supply, heating, ventilation, and air conditioning systems. Without adequate protection, a power failure, air-conditioning system failure or water leak might have catastrophic results for systems that are used to provide security.

Victoria Police should conduct risk assessments to determine the level of physical risk to a facility and the required security controls to be implemented.

The following guidelines should be considered when planning or evaluating a site:

- a) hazardous and combustible materials should be marked and stored in accordance with workplace safety requirements and located a safe distance from a secure area and from the site perimeter;
- b) emergency backup and redundancy equipment should be located in a safe position so as to ensure effective operation in the event of a disaster affecting the main site;
- c) appropriate emergency response equipment (such as fire fighting equipment) should be provided and suitably placed;
- d) perimeter walls and entry points should be strong enough to shield the facility from threats such as fire, explosion, and flood; and

Physical Security

- e) environmental conditions, such as temperature and humidity, should be monitored for conditions which could adversely affect the operation of information processing facilities.

Consideration should be given and appropriate action taken in relation to any security threats presented by neighbouring premises. For example, a fire in a neighbouring building, water leaking from the roof or in floors below ground level or an explosion in the street.

Supporting infrastructure services should be regularly inspected and as appropriate, tested to ensure their proper functioning and to reduce any risk from their malfunction or failure.

When ensuring continued electrical power services Victoria Police should consider:

- a) an uninterruptible power supply (UPS) that will enable continuous running (for a period of time), or provide the facility for a stable system shut-down. Contingency planning should identify response plans for a failure of the UPS;
- b) ongoing operation (beyond the capability of a UPS) that will be required for critical law enforcement data systems. An emergency generator and sufficient fuel and maintenance supplies should be considered for such situations; and
- c) the possibility of obtaining a continuous electricity supply via multiple providers to reduce the threat of failure as a result of a provider fault.

A failure in the water supply system may damage equipment or prevent fire suppression systems from functioning effectively. Sufficient water should be available to reliably supply supporting utilities such as air conditioning, humidification and fire suppression systems.

Backup support and supplies for supporting services, such as an uninterruptible power supply (UPS) or water reserves provide emergency services during a crisis and provide valuable assurance that security can be maintained during an emergency or crisis. Backup services should be planned, implemented, and tested regularly to ensure that they operate as expected. Such systems should have adequate supplies to operate the systems they are supporting for a pre-determined and accepted minimum period of time.

In order to ensure the continued availability and integrity of emergency and backup equipment effective regular maintenance should be conducted. The following guidelines for equipment maintenance should be considered:

- a) equipment should be serviced regularly and maintained in accordance with the supplier's or vendor's specifications;
- b) repairs, servicing and maintenance should only be conducted by trained and authorised personnel;
- c) where maintenance is performed by external personnel or performed offsite, consideration should be given to sensitive security-related or law enforcement data stored in the equipment. If appropriate, information should be cleared from the equipment or the maintenance personnel should be subject to a suitability test and background check; and
- d) all faults (real or suspected) should be documented and supported by preventive or corrective action.

Standard 17

Electronic communications infrastructure (wired or wireless) used for law enforcement data must be protected from interception or loss of service.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that electronic infrastructure (wired or wireless) be protected from interception or loss of service.

Statement of Objective

To ensure the continued availability, confidentiality and integrity of law enforcement data during electronic transmission.

Implementation Guidance

Computer networks provide numerous 'points of access' to Victoria Police information and law enforcement data. Whilst extremely useful in providing computing services distributed across Victoria Police, such networks also provide many possible access points that might be exploited by an intruder and used to illegitimately access or release law enforcement data and thus must be protected.

If an intruder is able to gain access to a communications cable carrying law enforcement data, there are numerous means by which they might be able to intercept (and read or steal) that data. Similarly, such cables can be damaged accidentally or intentionally sabotaged causing a disruption to law enforcement data flow. Network cabling should be protected from unauthorised interception or damage, for example by using a conduit or by avoiding routes through public areas.

Clearly identified cable and equipment markings (including cable termination points) should be used to minimise handling errors, such as accidentally connecting unauthorised users to law enforcement data or systems.

Physical network infrastructure that is used to connect computers to networks and systems such as patch panels and cable rooms should only be accessible to authorised people.

Physical network infrastructure, including architecture and configuration of patch panels, should be documented. Standard operating procedures should include the requirement for keeping such configuration documentation up to date when configuration changes are made.

For sensitive or critical systems further controls to consider include:

- a) controlled access to patch panels, cable rooms or access points used for inspection and maintenance;
- b) the use of secure conduit or securely routing the cables through protected areas;
- c) protecting the cable from interception via the use of electromagnetic shielding;
- d) the implementation of alternative transmission technologies such as fibre optic cabling (which is more complicated to intercept) where secure routing cannot be assured; and
- e) conducting technical and physical inspections for unauthorised devices being attached to the cables.

Physical Security

Law enforcement data travelling over cables can be compromised by interference from electrical power cables. To ensure continued access, data or communications cables should be segregated from electrical power cables.

All computing devices produce unwanted electromagnetic emanations that in certain cases can relate to the information being processed. Using specialised monitoring technology an intruder might be able to intercept the emanations of a computer display screen (monitor) and visually 'eavesdrop' on the information being processed. Emanations security (also known as TEMPEST) controls should be considered in accordance with Commonwealth protective security requirements.

Wireless communications enable computers to connect to networks without physically connecting (without wires). As such, the chances of being illegally intercepted by unauthorised persons are greatly increased. When implementing wireless communications infrastructure, a risk assessment will greatly assist in identifying and addressing security issues and reduce exposure.

Standard 18

Appropriate physical security measures must be implemented to protect all forms of law enforcement data during storage, handling and transport.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to ensure that appropriate physical security measures are implemented to protect all forms of law enforcement data during storage, handling and transport.

Statement of Objective

Law enforcement data must be protected during storage, handling and transport to control the risk of unintended loss or disclosure.

Implementation Guidance

In the course of operational and administrative duties, Victoria Police regularly handle large amounts of law enforcement data. In electronic form, data is provided with technical security controls, such as network logon accounts and passwords, to assist users in keeping the data secure. Law enforcement data also exists in hard copy printouts, official notebooks, police diaries, running sheets, court briefs, files and hand-written notes, whiteboards and other displays. Such 'hard copy' law enforcement data requires comprehensive and systematic security controls to ensure the information is adequately protected.

When information is being stored and not in use:

- a) Appropriate containers or filing cabinets should be used to hold law enforcement data. Containers holding particularly sensitive law enforcement data should be lockable and resistant to unauthorised entry.
- b) Consideration should be given to holding law enforcement data behind multiple physical barriers. For example, particularly sensitive law enforcement data could be stored in a locked cabinet in a locked room in a restricted office.

Standards and Protocols

Physical Security

Law enforcement data should only be handled by authorised personnel with a legitimate operational need-to-know. Personnel in possession of law enforcement data should ensure that:

- a) the data is made available to authorised personnel with a need-to-know;
- b) the data is not provided to personnel without a need-to-know; and
- c) there is no opportunity for unauthorised personnel to gain access to the data.

Work areas should have end of day procedures to ensure that law enforcement data is not easily accessible when the work area is unattended, including clear desk and screen policy (see Standard 19). Such procedures may include requirements for:

- a) ensuring there is no law enforcement data left on desks or tables;
- b) ensuring there is no law enforcement data left in unsecured bins;
- c) removing law enforcement data from whiteboards and other displays (special care needs to be taken with electronic whiteboards);
- d) locking containers (such as vaults and filing cabinets);
- e) ensuring keys to containers are secure; and
- f) locking windows and doors.

Personnel should avoid printing out or making copies of law enforcement data unless required for operational purposes.

Particularly sensitive law enforcement data should only be transported when enclosed in appropriate envelopes or containers. Victoria Police should have policy that provides guidance for choosing containers that:

- a) prevent unauthorised access to the data;
- b) reveal attempts to gain unauthorised access; and
- c) as much as possible, protect the enclosed law enforcement data from damage.

Transport of particularly sensitive law enforcement data may require additional accountability. Such accountability may be provided by signed and dated receipts or other notification of receipt.

Protection of nationally classified information requires specific storage, handling and transport procedures. This matter is dealt with in *Chapter Ten – Security Classified Law Enforcement Data*.

Physical Security

Standard 19

Victoria Police must implement a clear desk and screen policy for all environments that work with law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to implement a clear desk and screen policy for all environments that work with law enforcement data.

Statement of Objective

To reduce the risks of unauthorised access, loss of, and damage to law enforcement data in the workplace during and outside normal working hours.

Implementation Guidance

As law enforcement data is always subject to the 'need to know' principle it is important that when not in use it is protected from casual viewing by unauthorised personnel. Workplaces regularly host numerous visits from staff and personnel not directly involved in the same task and this should always be considered when working with law enforcement data. When implementing a clear desk and screen policy Victoria Police should consider that:

- a) sensitive or critical business information be locked away (ideally in a safe or cabinet or other forms of secure container) when not required, especially when the office is vacated;
- b) law enforcement data includes information displayed on computer screens, walls and whiteboards, and must be guarded from unauthorised viewing;
- c) computers and terminals be left logged off or protected with a screen and keyboard locking mechanism when unattended and be protected by key locks, passwords or other controls when not in use;
- d) mail collection and delivery points and unattended facsimile machines be protected;
- e) unauthorised use of photocopiers and other reproduction technology (for example, scanners and digital cameras) be prevented;
- f) documents containing sensitive or classified information be removed from printers immediately;
- g) computer systems be configured to only permit printing to local (workgroup) printing devices. Users should not be able to print to remote networked printers by default, where the printed material cannot be readily accessed by the person either printing the information or authorised to receive it; and
- h) at Approved Third Party workplaces, authorised users of law enforcement data typically represent a very small percentage of staff. Where possible Approved Third Parties should segregate equipment that provides access to law enforcement data (including printers) from general work areas.

Chapter Six – Remote and Mobile Access

Definition

Remote and Mobile Access is any access to law enforcement data via an electronic link that goes beyond Victoria Police physical network infrastructure. This includes:

- a) any wireless communications used for law enforcement data, such as Mobile Data Network (MDN) and police radios (analogue or digital); and
- b) any instance of law enforcement data being accessed via networks that are not controlled by Victoria Police. Examples of such networks are those belonging to other government departments, commercial organisations, private homes or the Internet.

In this context a portable device is any device used for remote or mobile access, such as a laptop computer or radio.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 20

Victoria Police must implement security controls to protect law enforcement data being exchanged over radios, remote computers and other mobile devices.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to implement security controls to protect law enforcement data being exchanged over radios, remote computers and other mobile devices.

Statement of Objective

To implement appropriate and consistent security controls that protect against the risks of using mobile devices and their communication facilities.

Implementation Guidance

The nature of police operations means that it is not always possible to guarantee that information provided to members on patrol will not be inadvertently disclosed. In certain situations it may be difficult to avoid radio information being overheard by members of the public. Care should be taken to ensure that as much as is possible, information sent or received over radio is not heard by others. Moving to a more secluded location or ensuring that only a limited amount of detail is requested whilst still in ear-shot of others will often suffice. Similarly users with remote computer access should take all steps possible to prevent law enforcement data being viewed by others.

If there is a significant risk of unauthorised people viewing, hearing or otherwise receiving sensitive information, action to reduce the risk to acceptable levels should be considered. Such action may include:

- a) moving to a less crowded location (particularly if using radios);
- b) requesting only information that is absolutely critical to the activity being performed (further sensitive detail could be acquired later under more secure circumstances);
- c) positioning the device such that people cannot view or receive information from the device without drawing attention to themselves;

Remote and Mobile Access

- d) using the device for work that does not expose law enforcement data or other sensitive data; and
- e) not using the device.

Providing Standard Operating Procedures and training in remote or mobile access will significantly increase security awareness and arm users with strategies to protect law enforcement data.

There is also a requirement to protect certain system information (not law enforcement data) against disclosure. The disclosure of such information may indirectly expose law enforcement data. Such information includes:

- a) passwords;
- b) presence/use of two-factor authentication (such as hardware tokens or biometric authentication);
- c) information about Victoria Police network infrastructure; and
- d) any other information that may aid an unauthorised person in gaining access to law enforcement data.

Take measures to protect mobile devices from theft. Protection includes physical protection such as lockable containers, as well as procedural protection such as instructions not to leave mobile devices unattended.

Regularly back up mobile devices that store law enforcement data to ensure that Victoria Police do not lose law enforcement data as a result of device theft. Backups are best stored at a location physically separate from the device and protected with appropriate security controls.

Storage encryption for mobile devices that store law enforcement data will reduce the disclosure risk of law enforcement data resulting from device theft.

Implement appropriate security controls on mobile devices before using them for accessing law enforcement data.

Protect mobile devices before connecting them to any network that is not controlled by Victoria Police. In particular, mobile devices such as laptops or other general-purpose computers should be protected from targeted attackers (such as hackers) and untargeted attacks (such as viruses, spyware, and Trojan horses).

Protect the data connections between mobile devices and Victoria Police networks with:

- a) cryptographic controls to protect confidentiality;
- b) authentication controls to ensure only authorised users have access; and
- c) access controls to ensure only the minimum required law enforcement data is transferred to or from the mobile device.

Wireless networks pose unique security risks. The risk assessment when considering using a wireless network needs to take into account the following:

- a) certain wireless security protocols are immature and have known weaknesses;
- b) it is extremely difficult to establish a physical security perimeter to prevent eavesdropping or interception of transmissions;
- c) wireless networks inherit all the vulnerabilities of wired networks, and introduce additional vulnerabilities; and
- d) how to meet any security requirements for protecting classified law enforcement data.

Remote and Mobile Access

Standard 21

Secure remote access must be provided for all portable computing devices used for law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that secure remote access must be provided for all portable computing devices used for law enforcement data.

Statement of Objective

Portable computing devices that remotely access law enforcement data are subject to increased risk of unauthorised access. This standard identifies strategies that aim to reduce the risk to law enforcement data by securing the remote connections.

Protocol 21.1

Victoria Police must ensure that:

- a) portable computing devices may only be connected to the law enforcement data if:
 - it is a portable computing device approved by Victoria Police; and
 - it has been checked and certified virus-free by a Victoria Police-approved virus scan product;
- b) users are authenticated at the start of each session;
- c) users are given the minimum system access necessary to perform their duties;
- d) when accessing Security Classified Information, the remote user's computing device is Classified to the required level. For example, a document classified SECRET must not be viewed on an unclassified device or a device with a security classification less than SECRET;
- e) any data transferred is appropriately protected during transmission and at the remote user's end;
- f) each portable computing device has a nominated officer who is responsible for ensuring that all security requirements relating to the device are met;
- g) Victoria Police portable computing devices are only used for authorised purposes;
- h) the person who has been provided with a Victoria Police portable computing device is responsible for the equipment and the information it contains;
- i) Victoria Police employees, contractors and consultants do not transfer custody of a portable computing device to another employee until information that the recipient is not authorised to access is removed;
- j) individual users who store law enforcement data on any portable computing device are personally responsible for the secure and adequate back up and recoverability of that information; and
- k) devices containing law enforcement data are only to be connected to external or third party networks or systems (including the Internet) if appropriate security controls have been implemented.

Chapter Seven – Electronic Data Storage Devices

Definition

Electronic data storage devices hold law enforcement data in digital or analogue form. Examples of devices that may hold law enforcement data in digital format are hard drives, USB flash drives, floppy disks, CDs and DVDs. Examples of analogue devices that may hold law enforcement data are magnetic tape devices such as audio and video cassettes.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 22

Victoria Police must ensure the effective removal of law enforcement data from electronic data storage devices when the data is no longer required. If effective removal cannot be ensured, the storage device must be destroyed.

Victoria Police must ensure that Agreements with Approved Third Parties establish requirements for effective removal of data or destruction of electronic data storage devices that have been used to store law enforcement data.

Statement of Objective

To reduce the risk of previously stored law enforcement data that is no longer required being accessible to unauthorised persons.

Implementation Guidance

The process of effectively removing data from electronic data storage devices is called sanitisation.

At a minimum, files containing law enforcement data held on electronic data storage devices should be deleted before being accessed by unauthorised staff.

For particularly sensitive law enforcement data Victoria Police should consider tools (software or hardware) that are able to delete files or reformat electronic data storage devices such that data cannot feasibly be read or recovered. Electronic data storage devices containing security classified information must be sanitised in accordance with Chapter 4 of the *Australian Government Information and Communications Technology Security Manual (ACSI 33)*.

Deleting or erasing data from electronic storage devices does not always guarantee that the data cannot be found and accessed.

All law enforcement data must be effectively removed from computing devices leased to Victoria Police before the device is returned to the vendor. If effective removal of law enforcement data cannot be guaranteed, arrangements should be made for the destruction of the electronic storage devices.

Electronic data storage devices (such as read-only CDs or DVDs) that cannot have files effectively removed should be destroyed when they are no longer needed.

Electronic Data Storage Devices

Destruction of electronic data storage devices containing particularly sensitive law enforcement data must ensure that the device can no longer be used. Such destruction needs to ensure that the data is destroyed or unrecoverable. This usually involves incineration or shredding.

Disposal and destruction should only be performed by competent, trusted and authorised staff in a controlled environment. Where the sanitisation or disposal involves particularly sensitive law enforcement data the process of destroying and sanitising should be auditable and steps should be taken to ensure law enforcement data is not released.

When dealing with large numbers of electronic storage devices (such as computer hard drives) it may be more expedient and safer for all devices to be collected and disposed of securely, rather than attempting to separate out the sensitive items.

Certain types of data in isolation might not appear particularly sensitive but when combined with other data, inferences might be made which increase the sensitivity of the combined or aggregated data. When accumulating electronic data storage devices for disposal, consideration should be given to this aggregation effect, which may cause a large quantity of non-sensitive information to become sensitive.

Chapter Eight – Cryptographic Controls

Definition

Cryptography is a means of modifying data such that it is unreadable without authorisation. Encryption is the process of applying cryptography to make data unreadable and decryption is the reverse process of making encrypted data readable. Decryption requires a key that proves authorisation.

Cryptographic controls are services or techniques that use cryptography to protect law enforcement data from:

- a) breaches of confidentiality by interception;
- b) undetectable compromise of integrity; and
- c) repudiation (denial of authorship).

A cryptographic key is a parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can read the data, while an entity without knowledge of the key cannot. Cryptographic keys are commonly generated from text passwords, unique hardware IDs, biometric data, or random numbers.

A key management plan is a document that describes the procedures and personnel required to manage and maintain the keys of a cryptographic system. It should apply to a specific instance of cryptography or cryptographic control. Appropriate key management will reduce the risks associated with implementing cryptographic controls.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Cryptographic Controls

Standard 23

Victoria Police must implement cryptographic controls in accordance with Australian Government protective security standards. Cryptography must be implemented to protect law enforcement data that is Security Classified PROTECTED and above while in transit over a lower-classified network. Law enforcement data that is Security Classified IN-CONFIDENCE must also be protected by cryptography while in transit, but may be subject to an exemption if supported by documented formal risk acceptance.

Victoria Police must ensure that there is an Agreement with Approved Third Parties that includes the requirement to use cryptographic controls for law enforcement data in accordance with Australian Government protective security standards.

Statement of Objective

To ensure Security Classified law enforcement data is protected in accordance with Australian Government protective security standards. Australian Government protective security standards have been developed such that when implemented correctly they provide a level of assurance that the data is secure.

Implementation Guidance

Cryptographic technologies are commonly utilised across government and industry to protect the confidentiality and integrity of sensitive data. Such controls are broken down into two-categories 'Government' and 'Commercial' grades. Commercial grade solutions from reputable vendors are generally considered to provide effective security and many implement the same encryption algorithm or formula as required by government systems. Cryptography should always be considered as part of security controls for any network that requires some level of assurance that its data is secure.

For sensitive official government information, the Australian government has established a system of classifying information that places it into categories to enable users to quickly identify how to treat and protect the information. These categories include IN-CONFIDENCE, PROTECTED, HIGHLY PROTECTED, RESTRICTED, CONFIDENTIAL, SECRET AND TOP SECRET. More detail about this scheme can be found in *Chapter Ten – Security Classified Law Enforcement Data*.

Cryptography can be used to protect the confidentiality and integrity of law enforcement data. Law enforcement data that is Security Classified PROTECTED and above must be encrypted in transit over a lower-classified network in order to comply with Australian Government protective security standards. There may be some instances where the risk to IN-CONFIDENCE law enforcement data does not warrant cryptographic protection. Formal risk assessment will enable consistent and thorough identification of such instances.

Cryptographic Controls

When dealing with Australian Government Security Classified data, Government grade cryptography is mandated. Australian Government protective security standards require that:

- a) information classified as PROTECTED must be encrypted using a Defence Signals Directorate approved cryptographic protocol when in transit over an IN-CONFIDENCE network;
- b) higher assurance is required for PROTECTED information in transit over an UNCLASSIFIED or public domain network and for higher-classified information in transit over an IN-CONFIDENCE network;
- c) Commonwealth protective security standards require that all IN-CONFIDENCE data must be encrypted when in transit to another government agency over an UNCLASSIFIED or public domain network. Furthermore, such encryption must be in accordance with Commonwealth standards;
- d) when IN-CONFIDENCE law enforcement data concerning a private entity is sent to that private entity over an UNCLASSIFIED or public domain network, Victoria Police must encrypt the law enforcement data in accordance with Commonwealth standards; and
- e) if IN-CONFIDENCE law enforcement data is not encrypted in transit, or encrypted using Commercial grade approved cryptography, Victoria Police must ensure that:
 - Victoria Police and any external receiving party are aware of the risk;
 - Victoria Police and any external receiving party have accepted the risk; and
 - any accepted risk has been documented.

The risk of not adequately protecting the data should be assessed before law enforcement data is transferred and at any time the transfer arrangements change. Risk assessment for determining cryptography requirements for law enforcement data classified IN-CONFIDENCE and below covering ongoing communications should include:

- a) the sensitivity of the law enforcement data;
- b) the volume of law enforcement data;
- c) the frequency of the data transfer;
- d) the accessibility of the transit link to unauthorised access;
- e) the impact of cryptography on content inspection systems;
- f) how many people have knowledge of the data transfer; and
- g) any other factors deemed relevant by Victoria Police.

Cryptographic Controls

Standard 24

Where cryptography is used to protect law enforcement data, Victoria Police must support it with appropriate policy, key management plans, and implementation documentation.

Victoria Police must ensure that there is an Agreement with Approved Third Parties that encrypt law enforcement data, which includes the requirement to support all instances of cryptography with appropriate policy, key management plans, and implementation documentation.

Statement of Objective

To reduce the risk of keys being inadvertently lost, disclosed, modified, or misused. Key management policy and plans provide a framework for implementing procedures for handling cryptographic keys.

Implementation Guidance

Implementation of a policy on the use of cryptographic controls is necessary to maximise the benefits and minimise the risks of using cryptographic techniques, and to avoid inappropriate or incorrect use. A policy on the use of cryptographic controls should include the following:

- a) a framework for determining when cryptographic controls are to be implemented to protect law enforcement data;
- b) the type and level of risk assessment to be used to determine the strength of cryptography to be used in each instance;
- c) requirements for operational and key management plans for each instance of cryptography, including:
 - roles and responsibilities of Victoria Police personnel;
 - processes and handling procedures for cryptographic material;
 - periodic review requirements; and
 - accountability; and
- d) requirements for compliance with relevant standards and legislation.

Key management is a set of processes and personnel responsibilities governing the lifecycle of cryptographic keys, covering the following:

- a) generation of cryptographic keys, including procedures for using keying material such as passwords, hardware tokens, or biometric sources. Key parameters such as length and time-to-live should also be documented;
- b) registration of keys, including any access and security requirements for the key registry;
- c) distribution of keys, including authorisation for which people and systems can distribute and receive keys;
- d) installation of keys;

Cryptographic Controls

- e) usage of keys;
- f) protection of keys, including access control requirements and cryptographic protection of keys;
- g) storage of keys;
- h) archiving keys, including security requirements for the key archive;
- i) recovery of keys;
- j) deregistration and revocation of keys;
- k) destruction of keys, including independent verification if appropriate;
- l) replacement of keys; and
- m) compromised keys.

The key management plan should also address requirements across all stages of the key lifecycle, including:

- a) personnel requirements and access control – who can perform the key management tasks, under what circumstances, and with what authorisation and accountability;
- b) logging – what events and metadata is logged and security requirements for the log archive;
- c) auditing – who can access the key management log and any requirements for automated alarms or warnings on suspicious activity; and
- d) scheduling – when each process can be performed and under what circumstances.

Implementation documentation is a record of how a cryptographic solution has been implemented in a specific instance. It includes details of the algorithms, protocols and products. It may also include procedures and personnel requirements for maintenance and management of a cryptographic system beyond the scope of the key management plan. Implementation documentation is necessary to maintain continuity across staff change, and enable appropriate decisions to be made regarding future system development and standards compliance.

Technical components of the cryptographic control to be documented are:

- a) algorithm details, such as:
 - name and variant;
 - type (eg. symmetric, asymmetric, or hash); and
 - key/block length;
- b) protocol details, such as:
 - name and version;
 - configuration; and
 - firewall requirements;

Cryptographic Controls

- c) product details, such as:
 - name and version;
 - vendor;
 - contact details for support;
 - contractual support arrangements;
 - licensing arrangements;
 - configuration;
 - technical authorisation requirements for users; and
 - integration with other relevant application software, operating systems, and greater network infrastructure (such as firewalls and other content inspection based security controls); and
- d) logging configuration, including:
 - what events are logged;
 - what metadata is logged;
 - where logs are stored; and
 - access control of log storage;

Process and personnel components of the cryptographic control to be documented are:

- a) name, position, and contact details for critical personnel:
 - technical maintenance staff;
 - incident management staff; and
 - system sponsor and delegate(s);
- b) authorisation required to access, modify or remove the cryptographic control;
- c) authorisation and restrictions of users and user activity;
- d) controls implemented to enforce access restrictions; and
- e) auditing arrangements, including:
 - processes for audit;
 - authorisation of auditing staff; and
 - accountability of auditing staff.

Chapter Nine – Law Enforcement Data Systems Acquisition and Development

Definition

Acquisition of law enforcement data systems is the purchase of commercial products for use within Victoria Police.

Development of law enforcement data systems is the process of building and customising products to meet Victoria Police's requirements. The process of development encompasses all stages of building law enforcement data systems, including requirements analysis, specification, design, implementation, testing, deployment and maintenance.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data systems.

Standard 25

Victoria Police must ensure that appropriate security controls, based on requirements identified in a threat and risk assessment, are designed and built into new systems or when law enforcement data systems are being changed.

Victoria Police must ensure that Agreements with Approved Third Parties who develop or maintain systems that interface with Victoria Police law enforcement data systems, require the implementation of appropriate security controls in new system developments or enhancements.

Statement of Objective

To ensure that security is considered as an integral part of new and enhanced law enforcement data systems.

Implementation guidance

Effective management during the development of law enforcement data systems will ensure system security and integrity is effectively considered and implemented in the new system. All stages of law enforcement data systems (such as development, test, and maintenance) should be strictly managed to ensure that any defects or vulnerabilities are not present in the live production system.

Early identification of security requirements assists in the development of effective security. System requirements for information security and processes for implementing security should be integrated in the early stages of law enforcement data system developments.

When designing the way in which a new or modified data system will integrate with the Victoria Police ICT infrastructure, care should be taken not to adversely affect the security of the infrastructure, the other data systems, or the security of the new or modified data system.

All law enforcement data systems should have an identified executive sponsor who is ultimately responsible for the delivery and maintenance of the new system. Project/Program Managers should be appointed who are responsible to the executive sponsor for the operation and conduct of the project/system development.

Law Enforcement Data Systems Acquisition and Development

Through the Project/Program Manager, Executive sponsors should enforce procedures that ensure all changes implemented or migrated between systems are reviewed. Changes made to live systems should be subject to strict control, monitoring and verification requirements.

Project/Program Managers should ensure that during development, access to all law enforcement data systems is only available to people with an operational need for access. They should ensure that proposed changes are reviewed to prevent security vulnerabilities from being introduced.

Conducting a comprehensive Information System Threat and Risk Assessment (ISTRA) will assist in accurately identifying security requirements for law enforcement data systems. An ISTRA methodology template, suitable for use in the context of Victoria Police's information systems is available from Victoria Police Business Information Technology Services.

Following the conduct of an ISTRA, appropriate information security control measures and/or remediation strategies must be identified, implemented, maintained, and reviewed.

Subsequent, supplementary ISTRAs should be carried out when:

- a) changes in the environment potentially result in:
 - additional types of threats; and/or
 - higher levels of risk;
- b) changes in the sensitivity of the information being managed potentially result in:
 - additional types of threats; and/or
 - higher levels of risk;
- c) a major modification to the existing system is being planned; and/or
- d) it has been three years since the last ISTRA.

The results of the ISTRA should be documented in a System Security Plan (SSP). A SSP addresses the system risks identified during the ISTRA and incorporates relevant organisational policy, corporate functions and culture. An SSP details specific security services and facilities of the system and delineates system responsibilities and expected behaviour of all individuals who access the system. The SSP becomes the document against which the security of the developed system is managed. It provides the basis for ongoing monitoring, assessment, review and upgrading of system security controls. Every information system should have a SSP as part of the essential system documentation. SSPs are relevant not only to the development of new systems but also provide the security documentation reference for the developed system.

Templates, guidance and training for ISTRAs and SSPs are available from the Victoria Police Business Information Technology Services.

An 'instance' is a software program that is currently running. Multiple instances mean that there are several copies or versions of that program running simultaneously. This is often used in software development to allow a program to be used for different purposes (for example, one copy may be used for development and another may be used for testing). During development there is a risk of defects or security vulnerabilities being migrated from low sensitivity instances (such as development or test) to higher sensitivity instances (such as version control or live production systems).

Live production instances of particularly sensitive law enforcement systems should be configured so that no single person can make an undetected change. This could be implemented using a multi-stage migration process that requires action from multiple people and/or a change detection warning that is sent to a person without direct access to the system.

Law Enforcement Data Systems Acquisition and Development

A process should be established to ensure that any unaccounted changes or migrations are identified, investigated, and reversible. Change control is particularly important when a system is in current use. It allows modifications to be tracked and inspected, creating a log for auditing and a level of accountability for people with access to make changes. In cases where change control procedures can be corrupted or bypassed, additional logging or accountability should be seriously considered.

The risks of processing failures that may compromise security should be minimised through careful design and implementation of applications. Effective techniques may include:

- a) encapsulation of data behind verification functions (such as “get” and “set” functions), disallowing direct access to data;
- b) sequence protection procedures to prevent sequenced processes from running out of sequence or running after failure of prior processing;
- c) graceful error/exception handling; and
- d) protection against common vulnerabilities such as buffer overflows and code injection.

Independent verification processes should be documented and implemented to ensure system and data integrity, with all results being kept secure. Any discrepancies should be raised as alerts for immediate investigation. Verification processes may include:

- a) reconciliation of separate-but-dependent or related processes;
- b) validation of static (unchanging) data and program code by cryptographic hash or checksum;
- c) bounds and format compliance checking for system-generated data;
- d) validating software runtime parameters such as start/end time, owner/user, parent process; and
- e) a mechanism for immediately alerting responsible staff of exceptions or anomalies.

Once a new system is fully implemented, a Post-Implementation Review should be conducted. Lessons learned will be valuable in informing future support strategies and development activities. In relation to security, Post-Implementation Reviews should address application and development security and evaluate the implementation of the System Security Plan.

Law Enforcement Data Systems Acquisition and Development

Standard 26

Victoria Police must implement procedures to ensure security during the development and maintenance of law enforcement data systems.

Victoria Police must ensure that Agreements with Approved Third Parties who develop or maintain systems that interface with Victoria Police law enforcement data systems ensure security during the development and maintenance of those systems.

Statement of Objective

To reduce the risk of security vulnerabilities being introduced during software development and the risk of critical technical information being communicated to unauthorised people.

Implementation guidance

Development activities are subject to unique security risks that should be controlled in order to ensure the integrity of law enforcement data systems.

An appropriately senior individual should be clearly designated as responsible for security of the development process. This person should have the following responsibilities:

- a) ensuring the project risk assessment includes security risks to the development processes;
- b) ensuring that security controls are selected that address the identified security risks and reduce such risks to acceptable levels;
- c) ensuring the security controls are implemented as designed; and
- d) providing a point of contact for security concerns or reports.

The process of developing software consists of several stages. A typical development process will include:

- a) Scoping – determining the context of the software within the business, and establishing the required resources;
- b) Requirements gathering – establishing the business objectives of the software, functions, and users;
- c) Specification – determining the procedural means for fulfilling the objectives and functional requirements;
- d) Design – planning the technical architecture of (hardware and software) components;
- e) Build – creating, assembling, and configuring the software;
- f) Test – verifying that the software functions as specified and fulfils its requirements;
- g) Deployment – making the software available to its users; and
- h) Maintenance – applying ongoing updates, upgrades and modifications to software that is in current use.

Law Enforcement Data Systems Acquisition and Development

The use of 'live' law enforcement data or copies of law enforcement data (data sourced from, or intended for, operational systems) during testing and preparation for data migration activities is strongly discouraged and should be avoided where possible. The use of fabricated 'dummy' data or de-identified data (where identifying information such as people's names and addresses are substituted) is preferred.

There are exceptional circumstances where it is necessary for project staff to have access to live or copied law enforcement data. When this does occur, care should be taken to ensure that access to that data is strictly controlled and staff with a need to access the data are deemed suitable. Law enforcement data used in test systems remains law enforcement data and must be afforded all security controls detailed in these Standards. Any project staff with access to such data should understand their security responsibilities for confidentiality and appropriate usage.

No stage of development should be considered less sensitive than another and it is important that appropriate security is applied during all stages of software development, from scope and requirements definition through to deployment and maintenance. Compromise of any of these stages may allow vulnerabilities or weaknesses to be introduced, or remain undetected or unaddressed.

Security of maintenance tasks is just as important as for initial development. Maintenance often allows developers closer access to a live system without the same level of oversight and review as earlier development stages. This makes it easier to apply undetected changes or access information without authorisation.

Development materials, such as designs, source code, libraries, and test data, should be protected from unauthorised access and modification. Such protection may include:

- a) understanding the sensitivity of the development materials and using a classification system to identify the sensitivity. Highly sensitive development materials will be at least as sensitive as the aggregate of all law enforcement data held by the system and the external systems/databases potentially accessible to the system;
- b) separating development materials into logical groups, such that each group can have specific people identified that require access. Such groups may have different people who require read-write (modification) access to those who require read-only access; and
- c) control access such that only developers and necessary other staff should have access to development materials. Furthermore, specific groups of material should only be accessible to people who have a legitimate need for access.

In addition to the technical security controls established to protect development and acquisition, appropriate attention should be given to ensuring that the physical security of the area in which the work is conducted is appropriate and effective.

Developers and other staff who have access to software development material should be deemed trustworthy. People who will have access to highly sensitive development materials may require more comprehensive background screening.

Developers and other people who have access to development materials should understand that such materials are sensitive information and must not be communicated to people without a need-to-know.

Law Enforcement Data Systems Acquisition and Development

Processes should be implemented to detect and repair deliberate or accidental introduction of security vulnerabilities and software defects. Such processes may include:

- a) peer review, including walkthroughs of development materials;
- b) independent scrutiny of development materials;
- c) security-focussed testing (in addition to functionality testing);
- d) evaluation of suspected software defects which may affect security;
- e) review of common types of defects and implementation of processes to reduce the risk of further similar defects; and
- f) addressing security vulnerabilities which appear to have been deliberately introduced.

Consideration should be given to backups and continuity management processes to recover from damage to development materials.

Version control tools should be used to track changes to development materials and revert to previous versions. Where version control software can be corrupted or bypassed, changes to development materials should be independently tracked to enable reliable auditing.

Chapter Ten – Security Classified Law Enforcement Data

Definition

Security Classified Information is defined as information that, if compromised, could have adverse consequences. The Security Classification System is an organisation’s mechanism for protecting the confidentiality of information generated by it or provided to it. The security classification system is implemented by assigning protective markings, such as TOP SECRET. The protective marking not only shows the value of the information but also indicates the minimum level of protection it must be afforded to safeguard it from compromise.

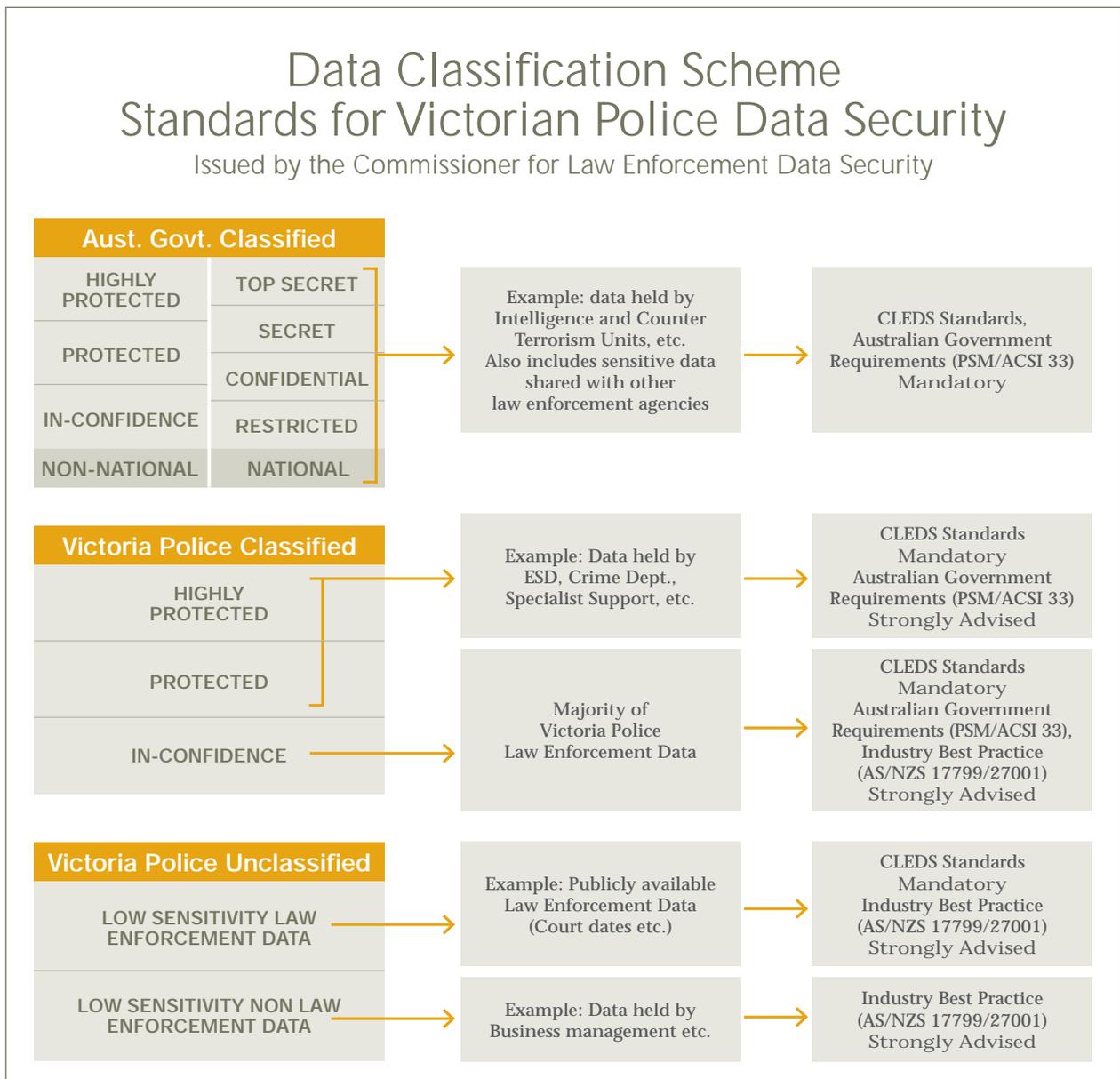


Figure 10.1 – Victoria Police Law Enforcement Data Classification Scheme

Security Classified Law Enforcement Data

Figure 10.1 illustrates the forms of classified law enforcement data that exist within Victoria Police, the likely location of such data and the requirement to implement Australian Government Protective Security controls.

Victoria Police law enforcement data requires a security classification to assist in its protection. Victoria Police assigns classification markings that align with Australian Government Security Classifications. With the exception of information that is non sensitive or publicly available, all law enforcement data is generally considered to have a minimum classification of IN-CONFIDENCE, with certain types of sensitive law enforcement data afforded higher Classifications.

Australian Government Security Classified Information is defined as official information that, if compromised, could have adverse consequences for the Australian Government. In the course of its duties, Victoria Police is often required to handle law enforcement data that is considered Australian Government Security Classified Information.

The Australian Government Protective Security Manual (PSM) provides the definitive policy for the security of Australian Government Security Classified information. As a State Government agency, Victoria Police are not required to comply with the PSM for law enforcement data owned and generated internally that does not impact national security. However, it is strongly advised that the PSM policy be used.

Victoria Police access, store and release certain types of information that is considered Australian Government Classified information. Typically, this information is generated by, or provided to, Victoria Police in relation to its work in counter terrorism or national intelligence activities. For Australian Government Security Classified information, implementation of the PSM and compliance with its strict controls is mandatory.

Australian Government Security Classified Information falls into two distinct categories:

- a) National Security Information – where the consequence of a compromise could affect the security of the nation (ie. its defence or its international relations). Victoria Police most often handle this type of information when dealing with national intelligence and anti-terrorist activities and when co-ordinating visits or events that involve foreign dignitaries; and
- b) Non-National Security Information – where the consequences do not threaten the security of the nation but rather the security or interests of individuals, groups, commercial entities, government business and interests, or safety of the community. The majority of sensitive law enforcement data handled by Victoria Police falls into this category.

National Security Information is afforded the following protective markings:

- a) RESTRICTED;
- b) CONFIDENTIAL;
- c) SECRET; and
- d) TOP SECRET.

Non-National Security Information is afforded the following protective markings:

- a) X-IN-CONFIDENCE (eg. 'STAFF' or 'SECURITY'-IN-CONFIDENCE);
- b) PROTECTED; and
- c) HIGHLY PROTECTED.

Security Classified Law Enforcement Data

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have, or require authorised access to Victoria Police or Australian Government Security Classified law enforcement data.

Standard 27

Victoria Police must establish clear and definitive procedures for the identification and classification of law enforcement data requiring confidentiality.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to establish clear and definitive procedures for the identification and classification of law enforcement data requiring confidentiality.

Statement of Objective

Law enforcement data requires confidentiality provisions where its unauthorised compromise or misuse could result in harm or damage to government, the public interest, private entities or individuals. By identifying a security classification for such data, Victoria Police will have an understood and agreed mechanism for immediately identifying the level of security required to protect that data.

Implementation Guidance

The person responsible for preparing the information must decide its security classification. This person is called the originator. When information is created, the originator must assess the consequences of damage from unauthorised compromise or misuse of the information. If adverse consequences could occur, the information must be security classified.

Security classified information should be kept to a minimum, where possible. Information requiring increased protection is identified by considering the consequences of its unauthorised disclosure or misuse.

Australian Government Security Classified information is any official resource (including equipment) that records information about, or is associated with Australia's:

- a) security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference;
- b) defence plans and operations;
- c) international relations, significant political and economic relations with international organisations and foreign governments; and
- d) national interest that relates to economic, scientific or technological matters vital to Australia's stability and integrity.

Not all information about these matters needs to be security classified. Information must only be national security classified if its compromise could damage national security.

Security Classified Law Enforcement Data

Non-national security information is any official resource (including equipment) that requires increased protection and does not meet the definition of national security information. Most often this will be information about:

- a) Victoria Police business where compromise could affect the Force's capacity to make decisions or operate or the public's confidence in Victoria Police;
- b) law enforcement operations where compromise could hamper or render useless crime prevention strategies or particular investigations or adversely affect personal safety; or
- c) personal information that is required to be protected under the Privacy Act, the Archives Act or other legislation.

The *Australian Government Protective Security Manual (PSM)* provides the definitive policy for the classification and handling of all official information (including law enforcement data). Victoria Police should refer to the PSM for detailed guidance on effective implementation of a Classification system.

Standard 28

Victoria Police must establish policy and protocols to ensure that all Security Classified law enforcement data is adequately protected. Australian Government Security Classified data must be protected in accordance with Australian Government protective security standards.

Victoria Police must ensure that Agreements with Approved Third Parties establish policy and protocols to ensure that all Security Classified law enforcement data is adequately protected.

Statement of Objective

To ensure that all Classified Law Enforcement Data is adequately protected and that where applicable, the minimum requirements mandated by Australian government protective security standards for protecting Security Classified information are implemented.

Implementation Guidance

It should be noted that these requirements apply to all forms of Security Classified law enforcement data including text, images, audio and video held on computing devices or in hard copy format or other storage media.

Security procedures are designed to increase protection during the use, storage, transfer or transmission and disposal of both paper-based and electronic Security Classified information. Access to Security Classified information is considered unauthorised if it is not:

- a) based on a legitimate 'need-to-know'; and
- b) sanctioned by government policy or agency direction; and
- c) an entitlement under legislation.

Security Classified Law Enforcement Data

The Australian Government Protective Security Manual (PSM) provides the definitive policy for the security of Security Classified information (including classified law enforcement data). The specific requirements to secure Security Classified information are extremely prescriptive and the complexity of controls is dependant of many circumstances. Victoria Police should refer to the PSM for detailed guidance on effective implementation of security for Security Classified law enforcement data.

As a State Government agency, Victoria Police is not currently obliged to comply with the PSM for law enforcement data owned and generated internally that does not impact national security. Due to the sensitive nature of classified law enforcement data it is strongly advised that the PSM be applied to Victoria Police Classified Data.

Standard 29

Prior to being granted access to Australian Government Security Classified law enforcement data, Victoria Police Employees, Contractors, Consultants and Approved Third Parties must meet Australian Government Personnel Security Clearance requirements for access to that data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to meet Australian Government Personnel Security Clearance requirements prior to being granted access to Security Classified law enforcement data.

Statement of Objective

To reduce the risk of unauthorised disclosure of Security Classified law enforcement data, Victoria Police must take all reasonable and appropriate precautions to ensure that only people with the appropriate security clearance gain access to it.

Implementation Guidance

It should be noted that the level of background checking required for access to law enforcement data described in *Standard 8* generally meets the Australian Government personnel security requirements for access to 'IN-CONFIDENCE' Security Classified information.

Minimum checking standards exist for every security clearance level. The purpose of the minimum standards is to ensure that security clearance procedures among all agencies who might share Security Classified information are consistent and that the resulting security clearances are portable between all agencies.

Due to the administrative burden and financial impost, security clearances should only be sought for individuals with a demonstrated need to know and requirement for regular access to Security Classified law enforcement data. Victoria Police should be aware that there are three types of temporary arrangements that provide limited access to Security Classified information. They are:

- a) limited higher access;
- b) provisional access; and
- c) emergency access.

Security Classified Law Enforcement Data

These arrangements are, by definition, temporary in nature and should be the exception rather than the rule.

The *Australian Government Protective Security Manual (PSM)* provides the definitive personnel security clearance policy for Security Classified information (including Security Classified law enforcement data). Victoria Police should refer to the PSM for detailed guidance on effective implementation of security clearances required for access to Security Classified law enforcement data.

Standard 30

When implementing security for the protection of Australian Government Security Classified law enforcement data and systems, Victoria Police must use Defence Signals Directorate (DSD) Approved Products (DAP) or solutions that are in accordance with Australian Government protective security standards.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to use DSD Approved Products (DAP) or solutions that are in accordance with Australian Government protective security standards for the protection of Security Classified law enforcement data.

Statement of Objective

The use of DSD approved products, solutions and configurations will assist Victoria Police in ensuring compliance with national security requirements.

Implementation Guidance

The Australian government has an evaluation scheme which details Information Technology products deemed suitable to adequately protect Government information, information systems and classified data. The selection of a Defence Signals Directorate (DSD) Approved Product (DAP) helps Victoria Police ensure that implemented technology provides adequate protection to Security Classified information.

The *Australian Government Information and Communications Technology Security Manual* (also known as ACSI 33) has been developed by the Defence Signals Directorate (DSD) to provide policies and on how to protect Information Communications Technology (ICT) systems.

When using Australian Government Security Classified information Victoria Police are required by the Protective Security Manual (PSM) to comply with ACSI 33. In accepting Security Classified information Victoria Police should consider the security implications of their ICT systems and devise policy and plans to ensure the systems are appropriately protected. Although security needs will be greatest when national security classified or non-national security classified information is being processed, even unclassified systems with no special safety, mission critical, or financial implications should have some degree of protection if a reliable or accurate service is to be maintained.

The DSD Evaluated Products List (EPL) provides consumers with a set of products that perform as claimed and supports agencies in their compliance with ACSI 33.

It should be noted that the selection and implementation of a DAP will not necessarily guarantee adequate security. Extreme care must be taken to ensure that the version and configuration of the product is in accordance with the detailed advice provided by DSD.

Chapter Eleven – Risk Management

Definition

Risk Management is a logical and systematic process of identifying, prioritising, treating, communicating and monitoring events that may prohibit an organisation from achieving its objectives, adversely impacting on the economic, effective or efficient delivery of its operations.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 31

Victoria Police must develop, document, implement and regularly review a risk management policy and process to effectively identify, analyse and treat security risks to law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement that they develop, document, implement and regularly review a risk management policy and process to effectively identify, analyse and treat security risks to law enforcement data.

Statement of Objective

To enhance Victoria Police's ability to safeguard the security of law enforcement data through the implementation of a comprehensive and effective information security risk management process that enables the identification and appropriate treatment of risks to the security of law enforcement data.

Implementation Guidance

The development, documentation, implementation and regular review of an effective risk management policy and process is essential to the creation of a secure environment for law enforcement data.

To ensure the successful application of the risk management policy it is critical that it is communicated to all staff who access law enforcement data in a form and manner that is relevant, accessible and understandable.

In general terms, Victoria Police's risk management process should be developed in the context of Victoria Police's strategic environment and its objectives, requirements and role.

For more specific information concerning the formulation, implementation and maintenance of an appropriate risk management process for law enforcement data, Victoria Police is directed to the Joint Australian/New Zealand Standard AS/NZS 4360:2004 on Risk Management. This document is widely regarded as an accurate and comprehensive description of the essential fundamentals of risk management.

Risk Management

Handbook 4360:2004 is the companion to AS/NZS 4360:2004 and is a useful guide to some aspects of the practical implementation of the principles laid out in AS/NZS 4360:2004.

Further information can be found at:

- a) Joint Australian/New Zealand Handbook HB 231:2004 on Information Security Risk Management Guidelines; and
- b) Standards Australia Handbook on Security Risk Management (HB 167:2006).

The Victoria Police information security risk management process should be documented as part of the Victoria Police risk management policy. The process should be complementary to and consistent with the Victoria Police information security policy and overall risk management strategy.

The policy should address all matters necessary to ensure that it provides a comprehensive guide to the appropriate management of risks to law enforcement data security, including:

- a) the objectives of, and rationale for, the policy;
- b) the links between the policy and Victoria Police's strategic and corporate business plans;
- c) the application of the policy;
- d) guidance on what may be regarded as an acceptable risk by Victoria Police;
- e) the allocation of responsibilities in relation to risk management; and
- f) the risk management process used by Victoria Police.

Chapter Twelve – Security Incident Management

Definition

Security incident management refers to response, recovery, reporting, and review of information security incidents and weaknesses. The standards in the chapter apply to security incidents that may affect law enforcement data.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 32

Victoria Police must establish, maintain and communicate reporting, escalation and response procedures for information security events and weaknesses that may affect law enforcement data.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to establish, maintain and communicate reporting, escalation and response procedures for information security events and weaknesses that may affect law enforcement data.

Statement of Objective

To allow timely corrective action to be taken in the event of an information security incident in order to protect law enforcement data and reduce the impact and likelihood of damage caused by a failure of information security controls.

Implementation Guidance

Information security incidents can range from minor problems and human error to major system malfunctions and criminal misuse of confidential information. An information security incident may include one or more events that may be related and together constitute a concerted attack or security failure. Examples of security incidents are:

- a) deliberate misuse of computer systems or information;
- b) accidental misuse or damage to systems;
- c) failure to comply with applicable policies or guidelines;
- d) physical security breaches (including trespass, failure of building security, and physical loss of data);
- e) unauthorised system changes;
- f) loss (or denial) of service, facilities capabilities or equipment;
- g) system malfunctions or other anomalous system behaviour;
- h) unauthorised access;
- i) malicious code; and
- j) false alarms.

Security Incident Management

A formal information security event reporting procedure, together with an incident response and escalation procedure, will set out the action to be taken on receipt of a report of an information security event. This point of contact for reporting information security events should be known throughout the organisation, always available and able to provide appropriate and timely response.

The reporting procedures should include:

- a) information security event reporting forms to support the reporting action and to help the person reporting to include all relevant response actions;
- b) the correct actions to be undertaken in case of an information security event, including:
 - immediately noting all important information about the event (for example, type of non-compliance or breach, occurring malfunction, messages on the screen, strange behaviour); and
 - not carrying out any own action, but immediately reporting to the point of contact.

A duress alarm should be considered for particularly high-risk locations and situations, where it may be valuable to discretely notify a responding group that a severe security incident is underway or has occurred. Response procedures should be appropriate to the high level of risk and the type of event.

All employees, contractors and third party users should be made aware of their responsibility to report any information security events or incidents that may apply to law enforcement data as quickly as possible. They should also be aware of the procedure for reporting information security events and the point of contact.

Information security incidents should be covered in general security incident response plans, which should detail procedures for:

- a) reporting
 - notification of the appropriate authority; and
 - identification and analysis of the incident;
- b) response
 - quarantine or separation from networks shared with live law enforcement data systems; and
 - communication with primary and secondary affected people (including staff, users, and people external to Victoria Police);
- c) recovery
 - collection of relevant evidence, if permitted by policy; and
 - restoration of normal operational services by rebuilding or replacing affected systems; and
- d) review
 - post-analysis and review of the incident; and
 - planning and implementing improvements to procedures and technology to prevent recurrence.

Security Incident Management

The incident response plan should include a framework for the collection and use of evidentiary material such as system logs for:

- a) incident diagnosis and analysis;
- b) use as forensic evidence; and
- c) supporting claims for compensation from suppliers for failure to meet service level agreements or terms of service.

Passwords and cryptographic keying material should be changed in response to a security incident.

The procedures set out in the security incident response plan should ensure that:

- a) live operational systems and data are only accessed with correct authorisation;
- b) all actions in response to the incident are documented and accountable;
- c) all action in response to the incident is reported to management and reviewed; and
- d) affected systems have their integrity confirmed and are restored to operational capacity as soon as is appropriate.

Where it is identified that evidence is to be collected for forensic examination (and possibly legal action), this should be done in accordance with Victoria Police standard procedures for collecting computer evidence from a crime scene.

Defence Signals Directorate may be able to provide assistance for:

- a) incident analysis;
- b) identification of remedial measures to remove the exploited vulnerability;
- c) minimisation of the likelihood of compromise; and
- d) overall assessment of Victoria Police's system security safeguards.

Security Incident Management

Standard 33

Victoria Police must establish a process for continual monitoring and improvement of information security incident management including a system for recording and post-incident analysis of information security incidents.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to establish a process for continual monitoring and improvement of information security incident management including a system for recording and post-incident analysis of information security incidents.

Statement of Objective

To ensure feedback on incidents and that information security incident management procedures can be continually improved so that future incidents are better managed.

Implementation Guidance

The information gained from the evaluation of law enforcement data information security incidents should be used to identify recurring or high impact incidents, and the likelihood that law enforcement data may be at risk from such incidents.

The evaluation of information security incidents may indicate the need for enhanced or additional controls to limit the frequency, damage, and cost of future occurrences, or to be taken into account in the security policy review process.

The requirement to restore systems and applications to normal operational capacity can conflict with the requirement to collect data for review and further response. Security incident response procedures should address this conflict.

Chapter Thirteen – Business Continuity Management

Definition

Business continuity management ensures that operational business can proceed in the face of threats to an organisation's business and provides a framework for building resilience and the capacity for an effective response to those threats.

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 34

Victoria Police must develop and implement business continuity plans to maintain or restore operations and to ensure availability of law enforcement data following interruption to, or failure of, law enforcement data systems or processes.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to develop and implement business continuity plans to maintain or restore operations and to ensure availability of law enforcement data following interruption to, or failure of, law enforcement data systems or processes.

Statement of Objective

To protect law enforcement data from the effects of major failures of information systems and to assist in recovery from interruptions to availability of law enforcement data or systems.

Implementation Guidance

The loss of law enforcement data or law enforcement data systems may be the result of natural disasters, accidents, equipment failures or deliberate actions.

A risk management approach should be taken to ensure information security aspects of business continuity are adequately addressed. This includes identification, assessment and evaluation of information security risks. Identification of risks should include information security implications for events (or sequences of events) such as fire, flood, theft, terrorism and equipment failure. Risk assessment should estimate the likelihood and consequence of such events.

In the development and implementation of its business continuity management process, Victoria Police should consider establishing:

- a) a methodology that provides an understanding of the risks to the availability of law enforcement data, including a method for the identification and prioritisation of critical business processes;
- b) a means of identifying all assets involved in protecting law enforcement data;
- c) an understanding of the impact that interruptions caused by information security incidents are likely to have on law enforcement data;

Business Continuity Management

- d) a framework for identification and consideration of additional preventive and mitigating controls;
- e) sufficient financial, organisational, technical, and environmental resources to address the security requirements of law enforcement data;
- f) guidance for the formulation and documentation of business continuity plans addressing law enforcement data security requirements; and
- g) a requirement that regular testing and updating of the plans and processes are put in place.

Victoria Police should ensure that the management of law enforcement data business continuity is incorporated in the organisation's processes and structure. Responsibility for the business continuity management process should be assigned at an appropriately senior level within Victoria Police.

Business continuity plans include:

- a) Identification of roles and responsibilities of all involved parties and personnel;
- b) identification of maximum acceptable level of loss of information and services;
- c) frameworks for determining the level of response to interruptions to business continuity;
- d) documented procedures to ensure business continuity in response to interruptions caused by disasters or loss of services; and
- e) alternative operational procedures to follow while affected information or services are unavailable.

Business continuity plans should be accompanied by:

- a) documentation of agreement and sponsorship by appropriate management;
- b) documentation and appropriate dissemination of business continuity procedures;
- c) education of staff; and
- d) testing and updating of plans.

The planning process should focus on operational requirements. For example, restoring access to law enforcement data in an acceptable amount of time. The required services and resources should be identified, including personnel and equipment, as well as alternate arrangements for information processing facilities.

Business continuity plans will contain sensitive information about Victoria Police that needs to be appropriately protected. Copies of business continuity plans should be stored in a remote location, far enough from the main site to be unaffected by most disasters. Remote copies of business continuity plans should be kept up-to-date and protected with the same level of security as at the main site. Other material or equipment necessary to execute the continuity plans should also be stored at the remote location.

The level of security at any temporary alternative locations should be equivalent to the main site.

Business Continuity Management

Standard 35

Victoria Police must regularly test and update business continuity plans to ensure they are up to date and effective.

Victoria Police must ensure that Agreements with Approved Third Parties include the requirement to regularly test and update business continuity plans to ensure they are up to date and effective.

Statement of Objective

To ensure that business continuity plans are up to date and effective.

Implementation guidance

Everyone with responsibilities under any business continuity plans should be aware of the plans, their responsibilities and their role should a plan be invoked.

The business continuity plan test schedule specifies how and when each element of the plan should be tested.

Business continuity plans should be regularly tested to provide assurance that the plan(s) will operate in real life. Techniques for testing business continuity plans may include:

- a) talk-through/paper based exercises (discussing the business recovery response to various example scenarios);
- b) simulation of technical recovery procedures and recovery at an alternate site;
- c) tests of supplier facilities and services; and
- d) complete rehearsals.

These techniques should be applied in a way that is relevant to the recovery plan. The results of tests should be recorded and, where necessary, actions taken to improve the plans. Regular reviews of business continuity plans will help identify changes in operational practices that are not yet reflected in the plans. A formal change control process will ensure that regular reviews allow business continuity plans to be maintained and kept up to date.

Business Continuity Management

Business continuity plans may need to be updated when:

- a) new equipment is acquired;
- b) systems are upgraded; and
- c) there are changes in:
 - personnel;
 - addresses, telephone numbers or other contact details;
 - business strategy;
 - location, facilities and resources;
 - legislation;
 - contractors, suppliers, and key customers;
 - processes, including new or withdrawn ones; and
 - operational or financial risk.

Chapter Fourteen – Relationships between Victoria Police and Approved Third Parties

Definition

An Approved Third Party refers to an organisation or individual external to Victoria Police that has been granted direct access to Victoria Police law enforcement data repositories.

Application

These standards apply across Victoria Police wherever and whenever law enforcement data is accessed by an Approved Third Party. More detailed protocols may exist within different Victoria Police departments but must not reflect lesser standards than those mandated here.

These standards do not apply to contractors or consultants employed or engaged directly by Victoria Police.

Standard 36

Before providing access to law enforcement data to an Approved Third Party, Victoria Police must ensure that:

- the receiving organisation has been granted authorisation by Victoria Police;
- the receiving organisation has a demonstrated need for law enforcement data;
- the receiving organisation undertakes security measures at least equal to those taken by Victoria Police to secure the information; and
- all law enforcement data exchanged meets the requirements for release.

Statement of Objective

To ensure Approved Third Parties do not gain unauthorised access to law enforcement data. Victoria Police must require Approved Third Parties to undertake appropriate security precautions when handling law enforcement data. Approved Third Parties also need to ensure that service providers contracted to them are fully aware of the Third Party's security policy and guidelines.

Protocol 36.1

Victoria Police must establish a procedure for granting authorisation that enables external organisations to become Approved Third Parties, which must include the creation and maintenance of a central register of Approved Third Parties.

Relationships between Victoria Police and Approved Third Parties

Standard 37

Agreements must be established prior to the exchange of law enforcement data between Victoria Police and Approved Third Parties.

Statement of Objective

Agreements must be established for the exchange of all law enforcement data between Victoria Police and Third Parties. Agreements with Approved Third Parties involving accessing, processing, communicating or managing law enforcement data or information processing facilities containing law enforcement data must cover all relevant security requirements.

Protocol 37.1

Exchange agreements must include the following (where applicable):

- a) management responsibilities for controlling and notifying transmission, dispatch, and receipt;
- b) procedures for notifying sender of transmission, dispatch, and receipt;
- c) procedures to ensure traceability and non-repudiation;
- d) minimum technical standards for packaging and transmission;
- e) escrow agreements;
- f) courier identification standards;
- g) responsibilities and liabilities in the event of information security incidents, such as loss of data;
- h) use of an agreed labelling system for sensitive or critical information, ensuring that the meaning of the labels is immediately understood and that the information is appropriately protected;
- i) ownership and responsibilities for data protection, copyright, software license compliance;
- j) technical standards for recording and reading information and software;
- k) any special controls that may be required to protect sensitive items, such as cryptographic keys; and
- l) all matters necessary to give effect to the obligations of Victoria Police under the Standards and Protocols established under the *Commissioner for Law Enforcement Data Security Act 2005*.

Relationships between Victoria Police and Approved Third Parties

Standard 38

Formal exchange policies, procedures, and controls must be in place to protect the exchange of law enforcement data, applicable to all types of communication facilities.

Statement of Objective

To maintain the security of law enforcement data exchanged by Victoria Police and any Third Party. Exchanges of law enforcement data between organisations must be based on a formal exchange policy, carried out in line with exchange agreements, and must be compliant with any relevant legal requirements. Procedures and standards must be established to protect law enforcement data in transit.

Protocol 38.1

The procedures and controls to be followed when using electronic communication facilities for the exchange of law enforcement data must include the following:

- a) procedures designed to protect exchanged law enforcement data from interception, copying, modification, mis-routing, and destruction;
- b) procedures for the detection of, and protection against, malicious code that may be transmitted through the use of electronic communication facilities;
- c) procedures for protecting communicated electronic law enforcement data that is in the form of an attachment;
- d) policy or guidelines outlining acceptable use of electronic communication facilities;
- e) procedures for the use of wireless communications (where applicable), taking into account the particular risks involved;
- f) employees, contractors and any other users' responsibilities not to compromise Victoria Police, including through defamation, harassment, impersonation, forwarding of chain letters and unauthorised purchasing;
- g) use of cryptographic techniques in order to protect the confidentiality, integrity and authenticity of law enforcement data;
- h) retention and disposal guidelines for all law enforcement data, in accordance with relevant legal requirements;
- i) not leaving law enforcement data on printing facilities, such as copiers, printers, and facsimile machines, as these may be accessed by unauthorised personnel;
- j) controls and restrictions associated with the forwarding of communication facilities, such as automatic forwarding of electronic mail to external mail addresses;

Relationships between Victoria Police and Approved Third Parties

- k) requiring personnel to take appropriate security precautions, such as not to reveal law enforcement data by being overheard or intercepted when making a phone call by:
 - people in their immediate vicinity particularly when using mobile phones;
 - wiretapping, and other forms of eavesdropping through physical access to the phone handset or the phone line, or using scanning receivers; and
 - people at the recipient's end;
- l) not leaving messages containing law enforcement data on answering machines since these may be replayed by unauthorised persons, stored on communal systems or stored incorrectly as a result of misdialling;
- m) educating personnel to avoid the security risks of facsimile machine use, namely:
 - unauthorised access to built-in message stores to retrieve messages;
 - deliberate or accidental programming of machines to send messages to specific numbers;
 - sending documents and messages to the wrong number either by misdialling or using the wrong stored number; and
 - the page caches and store page functions in case of a paper or transmission fault, which will be printed once the fault is cleared.

Standard 39

Victoria Police must check the implementation of the Agreements with Approved Third Parties and monitor compliance.

Mechanisms must be established to ensure that alterations to Victoria Police or Approved Third Parties law enforcement data systems and/or their interfaces do not reduce the security afforded to Victoria Police by the Agreement.

Statement of Objective

In order to reduce the security risk posed to law enforcement data, measures must be taken to ensure that the security controls, service definitions and delivery levels included in the Approved Third Party service delivery agreement are implemented, operated, and maintained by the Approved Third Party.

Relationships between Victoria Police and Approved Third Parties

Protocol 39.1

Adherence to the information security terms and conditions of the agreement must be regularly monitored and reviewed. Management arrangements for information security incidents and problems must include:

- a) monitoring service performance levels to check adherence to the agreements;
- b) reviewing service reports produced by the Third Party and arranging regular progress meetings as required by the agreement;
- c) providing information to Victoria Police about information security incidents involving law enforcement data and reviewing this information by the Third Party and Victoria Police, as required by the agreement;
- d) reviewing relevant Third Party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to the service delivered;
and
- e) the method for the management and resolution of any identified problems.

Implementation Guidance

Authoritative guidance on implementing exchange agreements is found at AS/NZS ISO/IEC 17799:2006 (section 10.8.2) and is replicated as Protocol 37.1.

Authoritative guidance for the exchange of information using electronic communication facilities is found at AS/NZS ISO/IEC 17799:2006 (section 10.8.1) and is replicated as Protocol 38.1.

There are a number of ways by which compliance with an Agreement can be monitored. Depending on the circumstances, Victoria Police should choose a method that will be appropriate and effective in satisfying the security requirements of the Agreement.

Chapter Fifteen – Compliance

Definition

The design, operation, use and management of information systems is subject to statutory, regulatory and contractual security requirements, which Victoria Police and Approved Third Parties must meet.

Intellectual property rights include software or document copyright, design rights, trademarks, patents and source code licences.

Legislation directly related to information security, including access and release, includes the following Acts:

- *Information Privacy Act 2000*
- *Health Records Act 2001*
- *Police Regulation Act 1958: s.127A*
- *Public Records Act 1973*
- *Freedom of Information Act (Vic) 1982*
- *Road Safety Act 1986: s. 92*
- *Commissioner for Law Enforcement Data Security Act 2005*
- *Constitution Act 1975: s. 95*
- *Public Administration Act 2004*
- *Evidence Act 1958.*

Application

These standards apply to all Victoria Police employees, contractors, and consultants and any Approved Third Parties who by way of Agreement with Victoria Police have authorised access to law enforcement data.

Standard 40

All legal requirements relating to information security and Victoria Police's approach to meeting these requirements must be explicitly identified and documented. These documents must be reviewed and updated regularly.

Statement of Objective

To ensure that those who access law enforcement data have a sound knowledge of the legal requirements relating to access to, and release of, that data. This in turn ensures that breaches of any legal and security requirements or obligations are avoided or at least minimised.

The community has a right to expect that all personal and other information maintained by Victoria Police is kept strictly confidential, only used for official purposes and not subject to misuse or for personal gain.

Compliance

Protocol 40.1

The definition and documentation of relevant legal requirements and Victoria Police's approach to meeting these requirements must be included in its Information Security Policy and updated regularly.

Detailed standard operating procedures relating to individual legal requirements must be developed and provided to authorised users and updated regularly.

Awareness and knowledge of legal requirements relating to access and release of law enforcement data must be included in the information security awareness training provided to authorised users.

Victoria Police must develop and implement an organisational data protection and privacy policy. This policy must be communicated to all persons involved in the processing of personal information and be updated regularly.

To ensure that the privacy of individuals and the confidentiality of Victoria Police information is maintained, the management and handling of all law enforcement data must be in accordance with the following Acts and any other relevant legislation:

- *Information Privacy Act 2000*
- *Health Records Act 2001*
- *Police Regulation Act 1958: s.127A*
- *Public Records Act 1973*
- *Freedom of Information Act (Vic) 1982*
- *Road Safety Act 1986: s. 92*
- *Commissioner for Law Enforcement Data Security Act, 2005*
- *Constitution Act 1975 Section 95*
- *Public Administration Act 2004*

Standard 41

Victoria Police must implement appropriate controls to ensure compliance with legislative, regulatory and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software.

Statement of Objective

To protect the Victoria Police information network from potential exposure, attack or compromise due to insecure software through complying with intellectual property rights and the legal requirements for the use of proprietary software.

Implementation Guidance

Uncontrolled or illegal versions of software are not necessarily securely implemented nor do they receive security updates from the vendor. The operation of uncontrolled or illegal versions of software on a network potentially exposes the network to attack or compromise. Victoria Police should implement measures to ensure that only approved and authorised software products are

Compliance

installed and all installations meet with legal intellectual property and copyright obligations, including usage agreements, update schedules, and holding current and correct licences.

In seeking to ensure compliance with relevant copyright laws, Victoria Police should consider the controls detailed in AS/NZS ISO/IEC 17799:2006 (section 15.1.2) as outlined below:

- a) publishing an intellectual property rights compliance policy which defines the legal use of software and information products;
- b) acquiring software only through known and reputable sources to ensure that copyright is not violated;
- c) maintaining awareness of policies to protect intellectual property rights, and giving notice of the intent to take disciplinary action against those who breach them;
- d) maintaining appropriate asset registers, and identifying all assets that are subject to intellectual property rights;
- e) maintaining proof and evidence of ownership of licences, master disks, manuals etc;
- f) implementing controls to ensure that any restrictions on the maximum number of users permitted per licence, is not exceeded;
- g) carrying out regular checks to ensure that only authorised software and licensed products are installed;
- h) providing a policy for maintaining appropriate licence conditions;
- i) providing a policy for disposing or transferring software to others;
- j) complying with terms and conditions for software and information obtained from public networks, such as the Internet;
- k) not duplicating, converting to another format or extracting from commercial recordings (film, audio) other than permitted by copyright law; and
- l) not copying in full or in part, books, articles, reports or other documents, other than permitted by copyright law.

Further detailed instructions can be found in the Victoria Police Manual at:

206-5 (7)	User Responsibilities – software
207-5 (6.3)	Access, use, and management – additional user responsibilities
206-3	Information Privacy
208-1	Release of Information – general principles
208-8 (1)	Release of Victoria Police personal records

Compliance

Standard 42

Victoria Police must ensure that records containing law enforcement data are protected from loss, destruction and falsification, in accordance with statutory, contractual and business requirements.

Statement of Objective

This Standard aims to ensure the security of organisational records containing law enforcement data in accordance with statutory, legal and business requirements, so that they are adequately protected from loss, falsification or destruction.

Implementation Guidance

Some records need to be securely retained to meet statutory, regulatory or contractual requirements, as well as to support essential business activities. Examples include records that may be required as evidence that an organisation operates within statutory or regulatory rules, to ensure adequate defence against potential civil or criminal action, or to confirm the financial status of an organisation with respect to shareholders, external parties and auditors. The time period and data content for information retention may be set by national law or regulation.

Victoria Police should consider the categorisation of records by record type with details of retention periods and type of storage media. Examples of the former are, accounting records, database records, transaction logs, audit logs, and operational procedures. Examples of the latter are paper, microfiche, magnetic, optical. Any related cryptographic keying material and programs associated with encrypted archives or digital signatures (see Chapter 8, Cryptographic Controls), should also be stored to enable decryption of the records for the length of time the records are retained.

Data storage systems should be chosen so that required data can be retrieved in an acceptable timeframe and format, depending on the requirements to be fulfilled.

The system of storage and handling should ensure clear identification of records and of their retention period as defined by national or regional legislation or regulations, if applicable. This system should permit appropriate destruction of records after that period if they are not needed by the organisation.

The Evidence Act 1958 sets legislative requirements for the preservation, reproduction and admissibility of documentary evidence in judicial proceedings. In storing records of a potential evidentiary nature, consideration should be given to the relevant provisions of the act, in particular, *Part III—Proof of Documents, Proof of Facts by Documents and Document Unavailability*.

Further information regarding managing organisational records is provided in:

- *Public Records Act 1973*
- *Evidence Act 1958*
- *ISO 15489-1:2001 Information and Documentation – Records Management – Part 1*

Compliance

Standard 43

Victoria Police must establish a system of monitoring and audit to ensure compliance with the Standards for Victoria Police Law Enforcement Data Security, and Protocols for Access to, and Release of, Law Enforcement Data, issued by the Commissioner for Law Enforcement Data Security.

Part Three

CLEDS functions and powers

Under the *Commissioner for Law Enforcement Data Security Act 2005*, the functions of the Commissioner include the establishment of appropriate standards for the security and integrity of law enforcement data systems and of appropriate standards and protocols for access to, and the release of, law enforcement data, including, but not limited to, the release of law enforcement data to members of the public. The Commissioner is obliged under the Act to consult with the Chief Commissioner of Police in the development of the standards and protocols.

The Commissioner has the authority to conduct monitoring activities, including audits, to monitor Victoria Police compliance with the established standards and protocols.

Where the monitoring or audit process indicates a failure to comply with the standards and protocols, the Commissioner will make recommendations to the Chief Commissioner of Police concerning action required to remedy the non-compliance. Should non-compliance continue, the Commissioner will notify the appropriate body, such as the Privacy Commissioner or the Director of the Office of Police Integrity, for relevant action.

The Commissioner will also undertake reviews of any matters relating to law enforcement data security requested by the Minister or the Chief Commissioner of Police.

The Commissioner reports annually to the Minister for Police who is required to table the Report in Parliament.

Definitions

Access refers to the ability of an individual or organisation to directly retrieve or view law enforcement data or access a law enforcement data repository. The act of 'Accessing' means:

- a) viewing or retrieving law enforcement data; or
- b) retrieving data from law enforcement data repositories.

Note – For the purpose of these Standards, the viewing of law enforcement data that has been Released in an authorised manner is no longer considered access.

Access Control refers to a service or technique used to permit or deny access to law enforcement data, or law enforcement data repositories. It is used to define or restrict the rights of individuals or information systems to access and use data.

Access Control Policy means a collection of rules and requirements for Access to law enforcement data intended to protect law enforcement data against unauthorised access, destruction, use, modification or release.

Account means a unique identifier that links a Subject to any operations performed in an Information System or Computing Device. An Account may have information associated with it, such as a User ID, Account Profile and other user information.

Account Profile means a set of rules that determine what operations an Account can perform in an Information System or Computing Device.

Agreement means a written record of a mutual understanding between Victoria Police and a third party, contractor, consultant or Victoria Police employee. In the case of an Agreement between Victoria Police and an Approved Third Party with respect to that party's access to, and management of, law enforcement data, this may take the form of a contract or a Memorandum of Understanding. In either case, the Agreement must include a provision that gives Victoria Police the right to take such action as it deems appropriate if the Approved Third Party breaches the Agreement such that Victoria Police considers that the security of law enforcement data may be threatened.

Approved Third Party means an organisation or individual external to Victoria Police that has been granted direct access to Victoria Police law enforcement data repositories.

Authentication means the act of verifying the identity of a User attempting to Access an Information System or Computing Device.

Asset means any item that has a useful or valuable quality for Victoria Police purposes.

Authorised Access means Access to law enforcement data that is in accordance with the Access Control Policy.

Authorised Victoria Police Business Need means a need that is directly related to the performance of an official Victoria Police function.

Authorised Release means Release that is sanctioned by law or Victoria Police policy.

Business Application means an aggregate of Computing Device, software, and Information System that as a whole, delivers a service or services to Victoria Police employees.

Computer means a Computing Device.

Definitions

Computing Device means:

- a) any electronic device that interprets Data as instructions (see definition for 'Software'); or
- b) any device that is electronically connected to the above, such that it may exchange data; or
- c) any aggregate of (a) and (b) in any variety and number; or
- d) the aggregate of any physical component of a Computing Device and the software available to run on it.

This includes (but is not limited to) desktop PCs, peripherals (such as screens, keyboards, and mouse), Personal Digital Assistants (PDAs), some telephones, USB Flash Drives, digital music players (such as iPods), printers, scanners, and network infrastructure (such as routers and firewalls).

Consultant means a Third Party engaged by Victoria Police to provide it with professional advice on any matter.

Contractor means a Third Party engaged by Victoria Police to perform a contract relating to the provision of goods or services to Victoria Police.

Data see *Law Enforcement Data*.

Data Storage Device means any device that stores Data. Storage may be, but is not limited to, solid state memory (flash drives), magnetic (hard disk, floppy disk, tape), or optical (CD, DVD).

Data Repository means a place of storage of law enforcement data. Data repositories include law enforcement data held on computing devices, data storage devices, or in hard copy format, including but not limited to, files of written reports and correspondence, police diaries, official notebooks, running sheets and other data repositories. (See also definition of law enforcement data).

Destruction means the act of altering Information such that its original form cannot be recovered.

Device means any physical object, and the aggregate of any number and variety of physical objects, together with any associated Information. This includes, but is not limited to, Computing Devices and Portable Data Storage Devices.

Disposal means Destruction of Information, followed by moving the destroyed information off premises, typically to a waste disposal facility such as recycling plant, tip, or garden.

External Agency means a Third Party.

Facility means an object, device, building or place that provides a storage or processing service for law enforcement data.

Firewall means a Computing Device that joins two Networks and filters Data travelling between the two Networks.

Flash Drive means a Portable Data Storage Device that uses solid state memory as a storage medium.

Information Security means the preservation of confidentiality, integrity and availability of information; other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.

Information Security Event means an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.

Definitions

Information Security Incident: an information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Information Security Policy means a collection of rules and requirements in any one or more documents intended to protect the integrity and confidentiality of Information and, in particular, safeguard against Information being subject to Unauthorised Access, Destruction, use, Disposal, modification or Release. Victoria Police Information Security Policy is not confined to one document and exists in a variety of locations including the Victoria Police Manual, Chief Commissioner Instructions, and in published Policy documents.

Law Enforcement Data means any Information obtained, received or held by Victoria Police:

- a) for the purpose of one or more of its, or any other law enforcement agency's, law enforcement functions or activities; or
- b) for the enforcement of laws relating to the confiscation of the proceeds of crime; or
- c) in connection with the conduct of proceedings commenced, or about to be commenced, in any court or tribunal; or
- d) for the purposes of its community policing functions.

Such information includes text, images, audio and video held on computing devices or in hard copy format, or other storage media, including but not limited to, data relating to individuals or aggregated data, written reports and correspondence, memoranda, police diaries, official notebooks, running sheets and other data repositories.

Malicious Code means Software that has an unexpected behaviour. This includes, but is not limited to, Software that can compromise the confidentiality or integrity of Information.

Network means any aggregate of Computing Devices.

Network Gateway means an aggregate of Computing Devices that, as a group, join two Networks.

Personal Information means any Information relating to a person.

Physical Security means the physical protection of law enforcement data from unauthorised access, destruction, use, modification or release.

Portable Data Storage Device means a Data Storage Device that may be removed from a Computing Device and connected to another Computing Device. The interface with a Computing Device may be, but is not limited to, Universal Serial Bus (USB), IEEE1394 (Firewire), Optical (CD, DVD), or Magnetic (Floppy disk, Tape).

Privilege means a right that permits a Subject to Access Information.

Privileged Account means an Account that has greater Privileges than other Accounts.

Privileged Operations means any operations that may or should be performed by a Privileged Account. This includes operations not performed by a Privileged Account, but should be limited only to Privileged Accounts.

Protocol means a statement of requirements which must, at a minimum, be addressed in order to meet a prescribed standard. Standard operating procedures and business rules implemented to give effect to a standard should include and further describe matters contained in the relevant protocol.

Definitions

Release means any disclosure of law enforcement data.

Remote Access means any access to law enforcement data that is provided to authorised staff physically located outside their normal working environment or connected to Victoria Police systems via a portable computing device.

Risk means a combination of the probability of an event and its consequence.

Risk Analysis means a systematic process to understand the nature of, and to deduce the level of, risk.

Risk Assessment means the overall process of risk analysis and risk evaluation.

Risk Evaluation means the process of comparing the estimated risk against given risk criteria to determine the significance of the risk.

Risk Management means coordinated activities to direct and control an organisation with regard to risk.

Security Breach means the deliberate or unintentional misuse of law enforcement data or law enforcement data systems or an event or occurrence that constitutes a violation of these Standards or Victoria Police Information Security Policy. Security breaches may occur from a variety of sources including, but not limited to, system users (authorised and unauthorised), external intruders, other computer systems and software applications (internal and external).

Security Classified Information means official information that, if compromised, could have adverse consequences for Government. This Information has been subject to a security risk assessment and, as a result of that assessment, assigned a protective marking or security classification label. See *Security Classification System*

Security Classification System means the set of procedures for identifying official information whose compromise could have adverse consequences for Government. It is the Government's mechanism for protecting the confidentiality of information generated by it or provided to it by other governments and private entities. The security classification system is implemented by assigning protective markings (such as TOP SECRET, PROTECTED, etc). The protective marking not only shows the value of the information but also indicates the minimum level of protection it must be afforded to safeguard it from compromise. It should be noted that the Classification System applies not only to data but also to computing and storage devices.

Security Clearance means an administrative determination by a competent authority that an individual is eligible and suitable, from a security stand-point, for access to security classified resources.

Security Event see *Information Security Event*

Service Provider means a legal or corporate entity contracted to provide services to Victoria Police or a Third Party.

Software means Data that is interpreted by a Computing Device as instructions. This includes (but is not limited to) machine code, interpreted scripts, and macros embedded in documents. Software also refers to any aggregate of the above across any variety of forms and Computing Devices.

Standard provides mandatory general principles for initiating, implementing, maintaining, and/or improving the security of access and release to law enforcement data for Victoria Police to ensure adequate information security management.

Definitions

Subject means any Device or Person, or any aggregate of the above in any number or variety.

Sworn Member means a 'member of the force', as that term is defined in the *Police Regulation Act 1958* (Vic).

System generally means a group of elements, components, or devices that are assembled to serve a common purpose. However, in relation to these Standards, system refers to either an information technology system or a non-electronic data repository. In an information technology system, this refers to all hardware, software, networks, cables, peripheral equipment, information, data, personnel, and procedures that comprise a computer environment. While a non-technological system refers to all activities involved in performing particular function/s, a non-electronic data repository refers to repositories such as the Victoria Police official filing system or Sworn Members' police diaries, official notebooks, running sheets and other data repositories.

System Sponsor means the position or person who is responsible for the operation of the infrastructure or system and the development and implementation of procedures for the effective operation of the infrastructure or system.

Third Party means an organisation or individual that is external to Victoria Police. (See also definition of Approved Third Party)

Unauthorised Access means Access that is not in accordance with the Access Control Policy.

Unprotected means not provided with security mechanisms to prevent unauthorised access.

USB Flash Drive means a Portable Data Storage Device that interfaces with a Computing Device via Universal Serial Bus (USB) and stores Data on solid state memory (flash memory).

User Access Profile means an Account Profile.

User Activity means any operations performed by a User on an Information System or Computing Device.

User ID means a unique identifier that is used to identify and handle an Account.

Vendor means the creator or provider of goods or services to Victoria Police.

Victoria Police means 'the force', as that term is defined in the *Police Regulation Act 1958* (Vic).

Victoria Police Employee means any person employed by Victoria Police, including any:

- a) 'member of the force', as that term is defined in the *Police Regulation Act 1958* (Vic);
- b) person employed by Victoria Police pursuant to the *Public Administration Act 2004* (Vic); and
- c) police recruits.

