



# Baltimore Certificates On-Line

CAPL P03 (SP – PU) - Security Policy (Public)

Information in this document is subject to change without notice.

No part of it may be copied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior written permission from Certificates Australia Pty Limited.

Written and published in Sydney, Australia, by Baltimore Technologies Pty Limited.

Copyright © 1998 Baltimore Technologies Proprietary Limited,  
ACN 003 823 461.

All Rights Reserved.

---

# TABLE OF CONTENTS

<b>IMPORTANT NOTE ABOUT THIS DOCUMENT</b> .....	<b>II</b>
<b>AMENDMENT CERTIFICATE</b> .....	<b>IV</b>
<b>INTRODUCTION AND OVERVIEW</b> .....	<b>1</b>
1. PURPOSE .....	1
1. SCOPE OF THIS DOCUMENT .....	1
1. DOCUMENT STRUCTURE.....	1
4. AMENDMENT PROCEDURE.....	2
5. REFERENCES.....	2
<b>MANAGEMENT PROCESS</b> .....	<b>1</b>
1. RESPONSIBILITIES.....	1
1. ESTABLISHMENT.....	1
2. PUBLICATION.....	1
3. REVISION .....	2
<b>APPENDIX A — CERTIFICATES AUSTRALIA PTY LIMITED SECURITY POLICY (PUBLIC)</b> .....	<b>1</b>
INTRODUCTION.....	1
RESPONSIBLE USE.....	3
SYSTEM PROTECTION .....	5
ACCESS CONTROLS.....	10
SYSTEM INTEGRITY .....	12
NETWORK SECURITY .....	16
PHYSICAL ENVIRONMENT.....	17
OPERATIONS.....	17
TECHNOLOGY .....	18
DATA SECURITY.....	19
COMPUTER VIRUSES .....	20
PERSONNEL.....	21
LEGAL.....	21
AUDIT .....	22
ELECTRONIC MAIL .....	22
PORTABLE COMPUTERS .....	25
PRIVATELY OWNED COMPUTERS OR SOFTWARE.....	25

---

## IMPORTANT NOTE ABOUT THIS DOCUMENT

The information contained in this document is intended for Baltimore Technologies personnel charged with the management and operation of the Certification Authorities owned and operated as Certificates Australia Pty Ltd or Security Domain Pty Ltd (Baltimore Certificates On Line), those persons named as recipients or those persons nominated in the circulation list.

It may contain privileged and confidential information and if you are not the intended recipient you must not copy, distribute or take any action in reliance on it.

If you have received this document in error, please notify the author immediately by reverse charge telephone call and return the original to the sender by mail. You will be reimbursed for postage.

This Security Policy document has been produced in accordance with the general provision of the Commonwealth's policy and guidelines on the protection of information and information technology environments.

**Contact:**

General Manager CA  
Baltimore Technologies Pty Ltd  
level 5, 1 James Place  
NORTH SYDNEY NSW  
AUSTRALIA  
  
Tel:+61 2 9409 0300

The presence of the signature below indicates that Baltimore personnel charged with operating the Certification Authority Services on behalf of Certificates Australia Pty Ltd and Security Domain Pty Ltd will abide by the policies contained herein.

---

**(BCOL Representative)**



---

# INTRODUCTION AND OVERVIEW

## 1. Purpose

The purpose of this document is to:

1. define the Security Policy (Public) for Certificates Australia Pty Limited (CAPL);
2. provide an overview on how the security policy is:
  - i.) produced; and
  - ii.) published.

This document contains a copy of the Security Policy (Public) authorised for publication (attached as Appendix A).

## 1. Scope of this document

This document gives guidance on how the Security Policy (Public) is prepared and managed, furthermore how the Security Policy (Public) is published. The Security Policy (Public) contains CAPL security policy statements covering:

- physical security;
- logical security;
- operational security, including:
  - archiving and backup;
  - operations and support personnel;
- detailed policy documents, including:
  - System Security Plan;
  - Contingency Planning and Disaster Recovery Plan;
  - Software and Data Backup Plan.

A separate policy statement on privacy and the fair handling of personal information has been prepared and published.

## 1. Document structure

The document is divided into the following sections:

1. Introduction and Overview;
2. Management Process;
3. Appendix A - Certificates Australia Security Policy.

## 4. Amendment procedure

As new standards emerge, or policy matters are identified for improvement, this policy document will be amended.

The responsibility for amending this document rests with the General Manager - CA. The naming convention for amendment notices shall be:

YY            Indicating the year the amendment was issued;

XXX          Where XXX represents a sequential number beginning with 000.

## 5. References

- Gatekeeper (Commonwealth Government)
- System Security Plan
- Contingency & Disaster Recovery Plan
- Configuration Baseline - CAPL
- Recognised CAPL Gatekeeper compliant CP

---

# MANAGEMENT PROCESS

## 1. Responsibilities

The General Manager - CA is responsible for the:

- CAPL security policy;
- preparation, publication and communication of the Security Policy (Public).

The CAPL Policy Approval Authority (PAA) is responsible for endorsing and approving the publication of the Security Policy (Public).

All designated operational and support personnel are responsible for ensuring compliance with the Security Policy (Public).

Note: In the event of a conflict between a CAPL public policy and a detailed CAPL planning document, the plan shall prevail.

## 1. Establishment

Good management practice and Gatekeeper Accreditation criteria demand the production and commissioning of various security policies and plans.

In accordance with these requirements, a security policy designated “Certificates Australia Pty Limited Security Policy (Public)” has been prepared and will be made public.

Note: Only policies carrying the designator “(Public)” shall be made public, with the exception of Certificate Policy Statements.

## 2. Publication

This policy shall be published in accordance with the requirement for it to be made public. Unless otherwise stated by the General Manager - CA, it shall be published on the CAPL website at:

[www.certificates-australia.com.au](http://www.certificates-australia.com.au)

### 3. Revision

The CAPL PAA shall review this policy at regular intervals. At a minimum, it shall be reviewed whenever a decision is taken to change the configuration baseline of the CAPL service.

---

## APPENDIX A — CERTIFICATES AUSTRALIA PTY LIMITED SECURITY POLICY (PUBLIC)

The Security Policy (Public) for Certificates Australia Pty Limited (CAPL) appears below, and is published on the Certificates Australia website at:

[www.certificates-australia.com.au](http://www.certificates-australia.com.au)

### Introduction

Certificates Australia Pty Limited (CAPL) has established a Root Certification Authority (RCA) and corresponding PKI, within which it operates a number of Certification Authority (CA) services.

A fundamental concept underpinning the operation of a PKI is trust. Trust must be realised in each and every aspect of the service operation. Trust is viewed and defined by the impact of each of the following elements on the whole PKI:

- Physical environment;
- Standards;
- Operations;
- Technology;
- Personnel;
- Legal;
- Audit.

This document contains security policy statements describing the high level security requirements of the CAPL PKI for each of these areas. The CAPL PKI will operate in accordance with:

- recognised international PKI standards;
- Gatekeeper accreditation requirements.

### Security Philosophy

The overarching security philosophy for all CA services is “Prevention, Detection and Considered Response”. For the purpose of this policy, ‘Considered response’ means such actions as are justified having considered all the circumstances.

This philosophy means that the first aim of a CA service is to:

1. prevent any unauthorised action taking place;

2. detect and record any unauthorised action that has taken place;
3. take such action as may be required given the information available.

Protection of the CAPL PKI shall be rigorous in application, the “Defence In Depth” principle will be the prime security criteria for service operation in ensuring that physical, administrative, logical and legal barriers operate together to protect CAPL assets, including but not limited to:

1. A configuration baseline for CAPL shall be established and maintained.
2. A Security Verification Program shall be established to confirm the presence, operation and effectiveness of the approved system safeguards and controls.
3. Systems Operability Tests (SOTS) shall be established to prove the correct operation of the CA service within defined parameters.
4. The storage of operational records and access to those records shall be subject to appropriate security safeguards and controls.
5. A Critical Incident Recovery Team (CIRT) shall be established to ensure that any disaster or contingency response event is quickly identified, appropriate action taken and policy, procedural or system deficiencies rectified.

## Standards

The security of the overall system is based on:

1. Australian Communication – electronic Security Instruction (ACSI) 33 – “Security in electronic Information Processing Systems”;
2. Australian Communication – electronic Security Instruction (ACSI) 37 – “Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification”;
3. Supplement to Australian Communication – electronic Security Instruction ACSI 37 - "Certification Test Procedures for Information Systems Processing Highly Protected Data";
4. Information Technology Security Evaluation Criteria (ITSEC) E3;
5. Commonwealth Government’s Protective Security Manual;
6. Gatekeeper – “A strategy for public key technology use in the Government”.

## Responsible use

### Context

Access to Service Provider information holdings is a privilege granted by the Service Provider based on its judgement of a number of factors, including relevant legislation and contractual obligations, the requester's need to know, the sensitivity of the data involved and the possible risk of damage to or loss of the particular resource.

Service Providers therefore reserve the right to limit, restrict or extend access privileges to their information holdings.

Service Provider facilities and user accounts are owned by the Service Provider and shall be used for the related activities for which they have been provided. Service Provider resources shall not be used for other commercial purposes or non-PKI related activities without the prior written authorisation of the General Manager - BCOL.

### User Responsibilities

All authorised users have the responsibility not to misuse Service Provider resources and report any misuse or suspected misuse of Service Provider resources to the Security Administrator or General Manager – BCOL.

Authorised users should familiarise themselves with any additional responsibilities associated with the resource for which they have been authorised to use and should ensure that hardware resources under their control are protected from theft, damage, loss and unauthorised access.

### Misuse

Service Providers characterise the misuse of their resources and privileges as unethical and unacceptable and as just cause for invoking sanctions.

The misuse of Service Provider resources and privileges includes, but is not restricted to, the following:

1. attempting to modify or remove resources without proper authorisation;
2. accessing resources without proper authorisation, regardless of whether the resource in question is owned by the Service Provider;
3. attempting to test, bypass or defeat any security safeguards established to protect resources with the exception of system security testing procedures requiring the prior written authorisation of the Security Administrator;

4. circumventing or attempting to circumvent assigned resource limits, logon procedures or assigned privileges;
5. using resources for purposes other than those for which they were intended or authorised;
6. sending fraudulent computer mail, breaking into another user's mailbox or reading their mail without permission;
7. sending any fraudulent electronic transmission;
8. violating any software licence agreement or copyright;
9. harassing or threatening other users or interfering with their access to Service Provider resources;
10. taking advantage of another user's naivete or negligence to gain access to resources for which they have not been authorised;
11. encroaching on others' use of resources through such activities as sending excessive or frivolous messages or printing excessive copies etc.; and
12. disclosing or removing third party proprietary information.

## Sanctions

Where an authorised user has been found to have misused the resources to which they have been granted access and/or has performed activities prejudicial to the security of those resources, these actions shall be documented and passed to senior management, who may wish to take disciplinary action.

Sanctions against contract employees shall be in accordance with the terms and conditions of their contract.

Depending on the nature of the user's actions, sanctions may range from counselling, suspension of system access rights or ultimately through to dismissal and/or legal action.

## System Protection

### Confidentiality

#### Information to be processed

The CAPL RCA and CA process Certificate Requests. The information contained in Certificate Requests, in terms of the GPKA Endorsed CAPL Certificate Policy Statements for Gatekeeper Individual, Organisation and Employee Certificates, is “not considered to be confidential”.

The CAPL RCA and CA operate as Windows NT services, which means that service personnel will not in the normal operation of the system see the information that is being processed.

CAPL Service personnel may, in order to ensure the correct functioning or integrity of the system, check Certificate Request information contained in system logs such as the error log and audit log, and check Certificate Request information contained in the RCA or CA database.

Note that only authorised RCA or CA service personnel including the IT Security Manager are allowed to:

- enter the secure operating area unescorted;
- activate or terminate the operating system (i.e. Windows NT) on the platforms upon which the RCA and CA are resident;
- activate or terminate the RCA or CA Windows NT service;
- have access to the RCA or CA databases.

The CAPL RA processes Registration Requests and dispatches keys and Certificates. The information required for a Registration Request is used to populate a field in an X.509 Certificate, i.e. used to create a Certificate Request for the CAPL CA. While Proof Of Identity (POI) information collected during a registration interview is considered to be confidential information, this POI information is collected manually and is not entered into the RA software. The X.509 Certificate information processed by the CAPL RA is therefore, in terms of the GPKA Endorsed CAPL Certificate Policy Statements for Gatekeeper Individual, Organisation and Employee Certificates, “not considered to be confidential”.

While such information is not be considered to be confidential, it is nonetheless processed on a “need to know” basis and only RA operations personnel are allowed to see the information.

CAPL RA service personnel may, in order to ensure the correct functioning or integrity of the system, also check Registration Request information contained in system logs such as the error log and audit log, and check Registration Request information contained in the RA database.

Note that only authorised RA service personnel including the IT Security Manager are allowed to:

- activate or terminate the operating system (i.e. Windows NT) on the platform upon which the RA is resident;
- activate or terminate the RA;
- have access to the RA database.

The Private keys generated by the CAPL RA as part of the Registration process, which are delivered by floppy disk or e-mail, are considered to be confidential. Each Private key is protected by a Personal Identification Code supplied to the End User at the time of Registration. Authorised RA service personnel are not allowed to view Private keys in the clear, End Users are allowed to view their own Private Keys in the clear (but not another End User's Private keys) after importing them into their Client PKI Application. Note that the importation process requires the correct entry of the End User's PIC, and protects the End User's Private key in the Client PKI Application database through the entry of an End User password known only to the End User.

#### System documentation

The CAPL RCA, CA and RA used approved PKI products from Baltimore Pty Limited. System documentation and system software supplied on the installation CD is therefore widely available to various Baltimore development center and sales staff and to Baltimore clients generally, as well as being available to CAPL RCA, CA and RA operations staff, including the General Manger – CA and the IT Security Manager.

Public documents relating to the operation of the system, such as this document, relevant Certificate Policy Statements and Certificate Practice Statements, the Privacy Policy – Public, the Certificate Management Life Cycle Overview and the Business Continuity Plan – Public as well as the Root CA Hash are made freely available to the general public through being published on the Baltimore and Certificates Australia web sites.

Access to internal policy and procedural documents, such as the Protective Security Risk Review, System Security Plan, CA Operating Procedures and RA Operating Procedures is limited on a “need to know basis”. The following persons are allowed to see these documents:

- General Manager – CA;
- IT Security Manager;
- authorised RCA, CA or RA operations personnel;
- technical writers (full time employees and contractors);
- security auditors (internal and external).

#### **Other aspects of the system**

Proof Of Identity (POI) information collected during a registration interview is considered to be confidential information. Access is strictly limited to the following persons:

- IT Security Manager;
- authorised RA operations personnel;
- security auditors (internal and external).

There are no access restrictions on reading the CAPL X.500 Directory other than requests for Certificate information being restricted to a single name exact-match search function. Certificate information and CRLs are automatically written to the CAPL X.500 Directory by the CAPL CA software, this information may not be altered. Maintenance of the X.500 Directory is restricted to the CAPL System Administrator.

The Firewall configuration is considered to be highly sensitive information and is restricted to:

- IT Security Manager;
- security auditors (internal and external).

#### **Asset protection**

The following items are considered to be confidential information:

- Proof Of Identity information, requiring strict protection from unauthorised disclosure through physical separation from other records and being maintained under locked control at all times;

- internal documents such as the Protective Security Risk Review, System Security Plan and Firewall configuration, these require a high level of protection by being maintained under joint locked control at all times in a B class container.

## Integrity

### System information

Certificate Requests, and Certificate information within the RCA system, CA system and X.500 Directory may not be modified nor deleted by operations personnel.

Authorised RA operations personnel are allowed to add new Registration Requests to the RA system. Registration Requests entered into the RA system may not be modified nor deleted by operations personnel.

### System documentation

System documentation supplied by Baltimore is subject to change by Baltimore in the event of a new software release.

Other system documents, including public documents and internal policy and procedural documents, may be changed by technical writers or other nominated personnel (e.g. System Administrator for documents published on the Baltimore and Certificates Australia web sites) on the authorisation of General Manager – CA.

Documents published on the Baltimore and Certificates Australia web sites are protected from modification or deletion by the general public.

### System software

RCA, CA and RA software, including operating software and X.500 Directory software, may be changed only by the CAPL System Administrator, with the prior approval of General Manager - CA.

System maintenance of error and audit logs (i.e. deletion of obsolete files or entries) may only be performed by the IT Security Manager, with the prior approval of General Manager - CA.

The Firewall configuration may be changed only by the IT Security Manager with the prior approval of General Manager – CA.

### Asset protection

Trusted system elements must be protected to as near as possible to absolute prevention of compromise. Trusted elements comprise the:

- CAPL RCA Signing key;

- CAPL CA Certificate Signing and Protocol keys;
- CAPL RA Private key;
- CAPL AA Private key;
- CAPL AA archived confidentiality keys database.

A back-up and archiving plan, disaster recovery and contingency plan and business continuity plan shall be established to jointly ensure the recovery of these elements in the case of failure, and the continuation of services to End Users in the case of compromise.

## Availability

The CAPL RA is used for internal staff registration only. The priority of the availability of the CAPL RA is therefore an internal matter within CAPL.

If the CAPL RCA is not available to client CAs, or the CAPL CA is not available to client RAs, Certificate Requests will not be processed until availability is restored and this may delay an End User in being able to use their Client PKI Application. It is therefore important that such availability be maintained as specified in a relevant service agreement.

There are two levels of availability for the X.500 Directory as determined by individual client service agreements:

1. Standard – during normal business hours, i.e. 9:00 a.m. to 5:00 p.m. Monday to Friday, Australian Eastern Standard or Eastern Standard Summer time;
2. Premium – available under customer agreement that provides 7 days x 24 hours availability.

Inability to access the X.500 Directory during the times determined by a service agreement may prevent a Relying Party from being able to make an informed decision whether or not to rely upon a Certificate, it is therefore very important that such access be available during the times specified.

Inability to access the Baltimore or Certificates Australia web pages may prevent a Relying Party from being able to access a relevant Certificate Policy Statement or Certificate Practice Statement. Such an inability may prevent the Relying Party from being able to make an informed decision whether or not to rely upon a Certificate, it is therefore very important that access to these web pages be available during the times specified in a relevant service agreement.

### Asset protection

Because of the nature of a PKI hierarchy, an outage of RCA, CA or RA services will initially affect a very small percentage of the overall user population and therefore such an outage is not considered to be a HIGH or SIGNIFICANT threat to the system. CAPL's service target to restore a service outage is prescribed in individual service agreements, where no such target is specified, it shall be 48 hours.

### Subsidiary items

System data and computer resources, such as hardware and software used in the system, are owned by CAPL unless otherwise specified in a relevant contract, Certificate Policy Statement or Certificate Practice Statement.

General Manager – CA has overall responsibility for the integrity of the data and other resources.

The IT Security Manager is to allow or deny access to the system or particular data in it on the authority of the General Manager – BCOL.

The IT Security Manager has the responsibility for detecting security violations or compromises.

The General Manager – BCOL has the responsibility for conducting internal security reviews and the Government Public Key Authority (GPKA) has the responsibility for conducting external security reviews.

The security responsibilities of individual users are defined in *Responsible Use* and in *Personnel*.

## Access Controls

### Security Authorisation

All personnel requiring access to Service Provider confidential information and / or Service Provider resources:

1. must be authorised by the Security Administrator;
2. shall be vetted by the Australian Security Vetting Service.

The Security Administrator has the responsibility of arranging the vetting of staff as required.

### User Identifier and Passwords

Certificates Australia and the Security Administrator shall ensure that:

1. Access to information is granted only to persons who have a work-related need for such access;
2. Users are informed that they are accountable for misuse of their access rights;
3. Logical access controls and procedures, such as for the use and management of passwords, are in place;
4. procedures are adopted which allow allocation of unique user identifiers, avoiding the need for shared identifiers; and
5. Service Provider audits are periodically conducted to determine the level of user compliance.

Authorised users shall ensure they observe all approved procedures and practices set down in relation to the usage of passwords.

### **Access Administration**

Responsibility for the administration and maintenance of all security access controls external to Service Provider platforms (e.g. Firewall) shall lie with the Security Administrator.

Access profiles shall be altered on a timely basis so as to reflect staff commencements, movements, absences and terminations.

Access to privileged functions shall be kept to a minimum number of staff. Special rights granted to individuals in positions of trust (privileged users) shall be reviewed periodically by the General Manager – BCOL. The period between reviews shall be dependent upon particular operational events, but shall not exceed twelve months.

### **Security Audit Trails**

Service Provider platforms shall incorporate audit trails to log those events of a security nature which are considered relevant by the Security Administrator. The following time-stamped events shall be recorded as a minimum:

1. all logon events, whether successful or not;
2. all attempts to access protected resources, whether successful or not;
3. all activities relating to the use of special system privileges;
4. all modifications to security information (user IDs and passwords);  
and

5. all modifications to system control parameters.

Such audit logs shall be reviewed regularly by the Security Administrator to identify any misuse of access privileges or attempts to do so. Logs are to be kept for a minimum of three years.

## System Integrity

### Software Change Control

In the context of this policy, “system software” relates to the technologies used to support the PKI functions through manipulation of the associated data holdings, and includes both commercial off-the-shelf and contractor or in-house developed software.

Access to and manipulation of production information holdings by a process or by an authorized user shall be through programs in “production status”, which shall be stored in protected file directories.

For the implementation of changes to system software:

1. the change shall be initiated by a duly authorised request;
2. the impact of the change, both technical and business, shall be assessed prior to the approval to proceed;
3. the change shall be approved in advance by General Manager – CA;
4. a record of all changes made shall be maintained by the Security Administrator;
5. appropriate training shall be identified and conducted prior to implementation;
6. system and user documentation shall be updated prior to implementation;
7. contingency provisions shall be established to ensure recovery from failure;
8. the time and manner of implementation shall be agreed between affected parties;
9. users of the software shall be notified, in advance, of the implementation details; and
10. there shall be formal acceptance of satisfactory completion by the system owner.

The change control mechanism shall be consistent across all Service Providers.

## Configuration Changes

Configuration changes are those changes to the baseline hardware, system software or associated packages in operation within the PKI or under the control of CAPL.

All proposed configuration changes shall maintain or enhance the level of system security and shall not, in any way, degrade existing levels of system security safeguards.

All configuration changes to Service Provider resources shall be recorded by the change control mechanism at each Service Provider location.

The General Manager - BCOL shall be notified of any configuration change.

## Software Testing

For software testing, there shall be an agreed testing specification defining:

1. the scope and type of testing and the level of testing to be applied;
2. the tests to be applied and the criteria for meeting those tests;
3. who shall undertake the testing;
4. who shall accept the results and the criteria required for acceptance.

Software testing shall be carried out in accordance with a testing specification and the testing specification, test data and test results shall be retained.

There shall be formal acceptance of satisfactory completion of testing by the relevant Service Provider owner.

Production data shall not be used for testing purposes unless all information identifying individuals, such as name, address etc, is first removed or modified in such a manner so as to protect that data from disclosure or reconstruction.

## Application Development and Maintenance

All application development and maintenance shall be undertaken within the framework of the following requirements:

1. all new applications systems shall have their data privacy, integrity and access requirements defined at the system definition stage; and
2. security requirements, including consistency with existing Service Provider control standards, shall be defined, specified and subsequently evaluated in any competitive process to select commercial of the shelf (COTS) software.

### Operating System Software

The implementation, modification and addition to all operating system software shall comply with the guidelines as outlined in *Software Testing* above.

### Contingency Planning/Disaster Recovery

Effective Disaster Recovery plans shall be maintained for all Service Provider computer systems. Such plans shall be kept as up to date as possible, tested and reviewed regularly under the direction of the General Manager – CA or delegate.

For each system, the system administrator shall ensure that:

1. security risks are identified and cost effective contingency and disaster recovery plans (and procedures where appropriate) are produced, tested and maintained to meet these risks;
2. staff under their control are trained in the appropriate contingency procedures;
3. backup and transaction logging procedures are sufficient for recovery purposes;
4. procedures exist for the transition back to normal processing.

The General Manager – CA shall ensure that a CAPL Contingency & Disaster Recovery Plan is established which includes:

1. disaster procedures for backup and archiving, sufficient for the restoration of the facilities and any critical applications;
2. guidelines for evaluating emergency situations and the determination of emergency requirements;
3. the establishment of an emergency response group with assigned roles;
4. plans for the provision of interim facilities, migration to those interim facilities and the return to normal processing;

5. procedures for data and software backup and recovery;
6. plans and procedures for the testing of contingency arrangements.

All staff affected shall be required to be aware of the contents of the Contingency & Disaster Recovery Plan and any tasks they have been assigned.

### **Backup and Recoverability of Application systems**

The backup of external Service Provider workstations and network file servers that are operated on client sites, shall be the responsibility of local staff, as authorised by the system administrator.

All Service Provider systems shall include support for full forward recovery so that minimal data is lost in the event of a system failure.

### **Software and Data Copyright**

Copyright laws limit the ways in which software and data can be used and breach of copyright can result in litigation.

Authorised software is software that has been legally obtained or developed, and used in accordance with any applicable conditions of acquisition.

Service Provider staff shall ensure that all copyrighted software and associated matter is used in accordance with the terms of the relevant licences.

System administrators shall ensure that mechanisms are in place to verify that only authorised software is in use. Such checks and procedures are to be performed at a frequency to reasonably satisfy General Manager – CA of the status of CAPL's software ownership.

The mechanism shall ensure compulsory deletion of any unauthorised software detected.

The Department shall ensure that authorised users are adequately advised of the requirements of this copyright policy, and the resulting procedures.

Authorised users shall ensure that they comply with software licensing agreements, particularly in regard to file copying and ensure that they refer any doubts concerning software validity to the system administrator.

## Physical Security of Computer Hardware

Procedures to ensure that all Service Provider resources are protected at all times from unauthorised access, theft, illicit use, illegal modification and intentional damage have been established. These procedures require all servers, modems, firewalls and diagnostic equipment to be located in secure, locked areas and access to this area be restricted to authorised personnel, or authorised maintenance technicians escorted by authorised personnel.

The requirement for these procedures shall extend to all locations where Service Provider resources are in use.

## Hardware/Software Servicing and Disposal

During maintenance visits by non-Service Provider personnel, an authorised staff member shall take responsibility for monitoring their activities. This staff member should have knowledge of the system sufficient to ensure that no breach of the security safeguards takes place during the visit. Any removal of diagnostic data or replacement of defective parts during a service visit shall be authorised by this staff member.

Service Providers shall ensure that all maintenance activity is appropriately logged.

Hardware that contains Service Provider data or software shall not be removed from Service Provider premises for repair unless the data is non-confidential or has been securely deleted.

Any Service Provider equipment shall be declassified or securely disposed of in such a manner that no confidential or sensitive information or system elements shall be accessible or retrievable from the equipment.

## Network Security

### General Network Security

In planning and implementing security safeguards for Service Provider communication needs, CAPL shall based its standards on those suggested in the Defence Signals Directorate (DSD) publication “Security in Electronic Information Processing Systems, ACSI 33”.

Physical access to Service Provider communication facilities shall be restricted to personnel authorised by General Manager – CA.

## Inter-network Security

No unauthorised external access to Service Provider resources shall be permitted.

CAPL shall establish an approved Firewall between Service Provider platforms and any public access network, such as the Internet.

Access from any external location shall be approved in advance by General Manager – CA, and shall only be approved when General Manager – CA is assured that the external access will not compromise existing security safeguards.

There shall be no access to external dial-in services such as bulletin boards, product user groups or support groups.

No data shall be downloaded from any external source. No mail services shall be supported.

Data received from external Service Providers (for example, certification requests) does not require encryption as it will not contain any confidential or sensitive information, but must be digitally signed.

## Physical environment

CA services are maintained in physically secure environments.

## Operations

CAPL has established a PKI that meets the Gatekeeper Accreditation standards.

Subordinate entities to the Root Certification Authority shall:

- conform to all CAPL PKI requirements;
- meet CAPL Policy Approval Authority requirements.

All private keys generated under the CAPL PKI shall be kept secret by their possessors and owners.

Key and certificate transport mechanisms shall ensure that only:

- lawful owners receive private keys and their associated certificates;
- authorised users receive public keys.

An X.500 directory is provided and maintained to facilitate access to:

- certificate status;

- public keys.

Planning documentation shall be prepared and maintained to ensure the correct operation of the service. The minimum documentation set includes:

- Concept of Operations
- Protective Security Risk Review
- System Security Plan
- Contingency & Disaster Recovery Plan

## Technology

The RCA, CAs and RAs within the CAPL PKI shall achieve Certification of underlying technology elements to the ITSEC E3 level, in accordance with:

- Gatekeeper Accreditation requirements;
- Section 23 of ASCI 33 – Multi Level Networks - Non-National Security Classified Systems.

The CAPL PKI shall operate under the general auspices of the Australian Communications-Electronic Security Instructions (ACSI) 33, which covers the following topics:

- i.) Preparation;
- ii.) The Environment;
- iii.) Technical Security;
- iv.) Security Audit and Review;
- v.) Network Specific Considerations;
- vi.) Small Systems Security;
- vii.) Miscellaneous Topics.

No member of staff shall:

- i.) use any CAPL service computers or network facilities without proper authorisation nor for unauthorised purposes;
- ii.) assist in, encourage, or conceal any unauthorised use, or attempt at unauthorised use, of any of the computers or network facilities;

- iii.) knowingly endanger the security of any CAPL service computers or network facilities, nor wilfully interfere with others' authorised usage.

## Data Security

### Categories of Data

Service Providers shall ensure that data under their control is classified according to its degree of sensitivity, confidentiality and criticality and shall be protected accordingly.

### Data Protection

All removable storage media, such as computer disks, tapes, CD-ROMS etc, that contain confidential information or trusted system elements shall be conspicuously marked to indicate the classification of the data stored therein. Disk, diskette and tape covers shall also clearly indicate the classification.

In general, data which is classified as "CONFIDENTIAL" or "COMMERCIAL IN-CONFIDENCE" shall not be stored on a local workstation unless protected by safeguards approved by the Security Administrator.

Shared data at these classifications shall be stored on a file server and shall not be stored on a user workstation hard disk. On a case by case basis, the Security Administrator may allow the storage of data at this classification on removable media which can be stored in an appropriate container when not in use.

Service Providers shall not extract operational data from corporate information holdings. Service Provider data shall be logically and physically separated from corporate information holdings.

### Reuse, Declassification or Disposal of Service Provider Storage Media

"Service Provider storage media" refers to magnetic tape cartridges and reels, PC Hard disks, diskettes, CD-ROMs and disk storage from other Service Provider equipment.

The System administrators shall ensure that when Service Provider storage media is reused or disposed of, there is no possibility of a breach of confidentiality through unauthorised access to any residual information contained on the media.

Service Provider storage media shall be disposed of in accordance with the highest classification of data it has ever contained and the degree of risk associated with a breach of data confidentiality at that classification.

Prior to disposal or declassification, no information contained on Service Provider storage media shall be deleted unless approved by General Manager – CA.

The General Manager – BCOL shall be responsible for providing an effective disposal service for Service Provider storage media.

## Data Transfer and Storage

Any Service Provider storage media used to transfer information shall not contain residual information which the recipient is not authorised to access. If the presence of residual data on used media cannot be determined, then new media must be used for the transfer.

These procedures shall be extended to all locations where Service Provider information is stored, including areas external to Service Provider premises (e.g. off-site storage locations for backup media).

Where the classification of material received from other Service Providers cannot be readily ascertained, the Security Manager shall determine the level of security required.

## Removal of Data from Service Provider premises

Information shall not be removed from Service Provider premises, either via a communication link, tape, disk, microfiche or other media unless authorised in advance by the Service Provider.

The Service Provider shall ensure that such data transfer is achieved via a method which ensures the confidentiality and integrity of the data being transferred.

## Computer Viruses

### Anti Virus Software

To reduce the risk of virus infection to operational resources, Service Providers shall implement safeguards to control the sources of possible infection.

Principal among these is the implementation of anti virus software and the Security Administrator shall approve any virus detection product(s) and procedures.

## Anti Virus Procedures

Service Providers shall establish procedures to protect against the introduction of viruses from external sources, either through equipment maintenance, transfer of information by magnetic media or by access to external networks.

The General Manager – CA shall ensure that virus detection software and procedures are provided to all Service Provider sites together with training in their use.

System administrators shall ensure that newly acquired software is subjected to virus detection checks using the approved virus detection product before use and ensure magnetic media used for data exchange between Service Providers, etc is virus scanned before use.

## Personnel

### Positions of Trust

Service provider operational positions, requiring access to the secure operational area, are designated as 'Positions of Trust'. Personnel shall not be permitted to assume Positions of Trust without due clearance by the Australian Security Vetting Service (ASVS).

### Education and Training

Training in security matters is an essential element in providing staff and contractors with the skills necessary to meet their responsibilities.

Service Providers shall provide ongoing training in security, addressing general responsibilities and basic security procedures affecting all staff. This shall include communicating the Security Policy to all existing and new users of its resources.

New security procedures shall not be introduced without a corresponding education program to ensure staff are aware of their new responsibilities.

## Legal

The contractual obligations, rights, and duties of each party in the PKI shall be identified in contract and reflected in Certificate Policy Statements, to ensure that the operation of the CAPL PKI is supported by a consistent legal infrastructure.

## Limitation of liabilities

CAPL has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to inhibit misuse of those resources by authorised personnel or fail to prohibit access to those resources by unauthorised individuals.

Such measures include the provision of a "no trespassing" message during system logon that stipulates that by continuing further, the person concerned:

1. is aware that the system is to be used by authorised Service Provider users only;
2. is, by continuing to use the system, representing that they are an authorised user;
3. as such, agrees to abide by the responsible use provisions as defined in this Policy;
4. is aware that their actions are being monitored by the specific userID assigned to them and the logs of such actions may be provided to law enforcement officials investigating any possible misuse of the system; and
5. is aware that, in this event, usage shall legally be considered to have been undertaken by the user assigned that identification.

## Audit

All CA services log security related or pertinent events. These logs are reviewed regularly to identify any attempted or actual security breaches, including misuse of access privileges.

## Electronic mail

### Usage

No e-mail services are provided on Service Provider operational platforms.

E-mail services may be provided on other workstations to Service Provider personnel at the Service Provider's expense to assist them in carrying out their day to day business. The e-mail system shall be used for business related purposes only and users shall treat all messages sent, received or stored in the e-mail system as business messages.

Should personnel make incidental use of the e-mail system to transmit personal messages, such messages shall be treated no differently from other messages and, as such, the Service Provider reserves the right to access, copy or delete all such messages for any purpose and to disclose them to any party deemed appropriate by the system owner.

Additionally, personal use of e-mail facilities shall not:

1. interfere with normal business activities;
2. involve any form of solicitation;
3. be associated with any for-profit outside business activity;
4. be used for the exercise of the user's right to free speech; and
5. potentially embarrass the Service Provider.

Unless it is encrypted, sensitive information shall not be sent via e-mail facilities.

Where they choose not to control the content of messages posted to a web site they establish or operate, Service Providers specifically disclaim any responsibility or liability for the contents of any information or message appearing on that web site. In this situation, the Service Provider is not required to verify the correctness, accuracy, or validity of the information appearing on the web site. Comments that users post to the web site shall be deemed as not necessarily formal statements issued by, or the official position of the Service Provider.

Service Providers reserve the right to censor any data posted to an electronic mail system, web site or any other electronic system they operate or control. In doing so, the Service Provider shall notify users of such facilities that the facilities are Service Provider business systems, and not public forums, and as such do not provide free speech guarantees.

Service Providers prohibit e-mail users from engaging in any communications which include, but which is not limited to, transmission of defamatory, obscene, offensive or harassing messages; or messages that disclose personal information without authorisation.

Authorised users shall not use an electronic mail account assigned to another individual to either send or receive messages. If there is a need to read another user's mail, such as in the case where a user is absent on leave, message forwarding and other facilities shall be utilised instead.

## Privacy Expectations

All e-mail messages sent over Service Provider telecommunications systems by users shall be deemed to be the property of the Service Provider and therefore not subject to expected individual privacy provisions. Authorised users of a Service Provider e-mail system shall have no expectation of privacy associated with the information they store in or send through these systems.

Notwithstanding this provision, authorised users shall treat electronic mail messages as private information and shall ensure that it is handled as a private and direct communication between a sender and a recipient.

To properly maintain and manage this property, Service Providers reserve the right to examine all data stored in or transmitted by these systems. Such right shall be given to the Security Administrator or delegate and shall be for the purposes of conducting a properly initiated investigation of suspected misuse of Service Provider resources or for the disposal or re-assignment of computer files belonging to an authorised user in the case when that user is no longer an authorised user.

Where a Service Provider provides computer networking services for a third party, the Service Provider shall be deemed as providing communications services, not message protection services. Accordingly, the Service Provider shall make no assurances relating to the privacy of that information and shall assume no responsibility for the disclosure of information placed on the network.

## Recording and Retention of Electronic Mail

Service Providers shall maintain a systematic process for the recording, retention, and destruction of electronic mail messages and accompanying logs. The process and the retention period shall be determined by the Security Administrator.

The destruction of both logs and the referenced electronic mail message shall be deferred whenever legal notice is received or when the possibility exists that such material is required for imminent legal action.

## Address Lists and Contact Numbers

Information regarding access to Service Provider computer and communication systems, such as dial-up modem phone numbers and e-mail address lists shall be considered sensitive information. This information shall not be posted to an external BBS, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the prior written permission of the information custodian.

## Portable Computers

### Usage

The responsibility for the protection of Service Provider portable computers, or corporate portable computers used by Service Provider personnel, and the data contained thereon shall reside with the person to whom the equipment has been provided.

When used to process sensitive data (i.e. “CONFIDENTIAL” or “COMMERCIAL IN CONFIDENCE”), portable computers shall have a security safeguard installed which requires a user to enter a password before access is granted to data stored on its hard disk. All sensitive data on the hard disks shall be encrypted.

A portable computer shall not be connected to a Service Provider platform for other than diagnostic or testing purposes and shall only be so connected:

1. with the prior written approval of General Manager – BCOL
2. after it has been checked and certified virus free by a virus scan product approved by the Security Administrator for that purpose.

Personnel shall not transfer custody of a portable computer to another officer until all sensitive data contained on its hard disk is erased or declassified.

Portable computers shall be kept secure at all times and shall be placed in locked cabinets when not in use or left unattended for any length of time.

## Privately owned Computers or Software

### Usage

The use of computer equipment owned by Service Provider, contract or vendor personnel to access Service Providers holdings shall not be permitted. No exceptions to this rule will be allowed.

No privately owned equipment shall be connected to Service Provider processing systems. No exceptions to this rule will be allowed.

No privately owned removable media shall be used in connection with Service Provider processing systems. No exceptions to this rule will be allowed. Privately owned removable media should not be used in connection with personal computers in the custody of Service Provider personnel. Where circumstances arise mandating the use of privately owned removable media, such media shall be virus scanned using the approved Service Provider virus scan product before its use.

The use of non-Service Provider software on Service Provider resources including games and screen savers, is strictly prohibited.