VeriSign Australia Limited

VSA Security Policy V1.51

The controlled master of this document is held in electronic form.
If this is in printed form it is an uncontrolled copy.

DOCUMENT CONTROL

Preparation

Action	Name	Date
Prepared by:	David Caldwell	26 September 2002
Reviewed by:		

Release

Change	Doc Version	Date Released	Change By	Description
0	1.0	10/1/00	D Caldwell	Base Document
1	1.1	7/3/00	D Caldwell	Amendments throughout
2	1.2	24/3/00	D Caldwell	Amendments throughout
3	1.3	27/9/01	D Caldwell	Amendments throughout
4	1.4	7/11/01	D Caldwell	Review and update as required.
5	1.5	4/10/02	D Caldwell	Rebranding to VeriSign Australia
6				

Document Properties

Document Name:	Number of pages:	Last Updated:
VSA Public Security Policy V1.51	52	4 October 2002

CONTENTS

1. Introduction

The purpose of this document is to define the Security Policy (Public) for VeriSign Australia Ltd.

This document sets out the guiding principles and policies used to establish the appropriate level of system and data availability, integrity and confidentiality used throughout the Certification Authority.

This document is a Public document and is able to be distributed and advertised freely.

1.1.   Scope of this document

This document describes how the VeriSign Australia Security Policy is prepared, managed and published.

This document contains statements pertaining to:

- Physical security

- Logical security

- Operational security

- Data backup and archiving

- Operational personnel

- Information privacy

- Detailed policy documents, including:

    o Information Systems Security Plan

    o Physical Security Plan

    o Disaster Recovery Plan

    o Software and Data Backup Plan.

    o Certification Authority Operations Manual.

1.2.   Amendment Procedure

This document will be reviewed on a regular basis to allow for amendment to areas identified as requiring improvement or that have undergone change. This includes where any alterations have been made to the standard

operational configuration of the CA and RA services provided by VeriSign Australia.

The responsibility for amending this document lies with the Security Manager.

1.3. Overview

VeriSign Australia has developed a Regional Operations Centre at 134 Moray Street, South Melbourne, for the purpose of providing Certification Authority (CA) and Registration Authority (RA) services.

In order to strengthen the extreme trust placed in VeriSign Australia to conduct this business it is necessary to demonstrate that the highest standards of trust and security have been put in place surrounding these services. These standards are reflected through the provision of the following:

- Secure physical environment,

- Policy and procedure,

- Technology,

- Experience,

- Audit,

- Personnel vetting,

- Legal expertise, and

- Operations.

This document contains security policy statements that describe the high-level security requirements of the VeriSign Australia RCA for each of the above elements.

As part of establishing worldwide recognition and trust, VeriSign Australia has achieved full accreditation with the Australian Commonwealth Government under Project GateKeeper [1]. This is a strategy initiated by the Australian Government, which "…***provides a structure through which the government can ensure quality, integrity, security and authenticity in the transmission of information and the transaction of business***." This strategy includes the establishment of standards for Public Key Infrastructure.

1 GateKeeper – A strategy for public key technology in the Government.

2. Security Philosophy

The approach to the implementation of security, in particular the physical concept, design and evaluation process adopted by VeriSign Australia, is based upon the philosophy that security is generated from three key fields. These are dependent upon each other and must therefore be compatible with each other.

2.1.   Management

Management refers to how the VeriSign Australia Regional Operations Centre (ROC) is controlled relative to security and the individuals involved in maintaining a secure environment, and their responsibilities/duties. Management of security must be considered the most important factor in ensuring a secure operational environment.

2.2.   Architecture and planning

This refers to the security that is provided by the way the Regional Operations Centre is constructed.   It further refers to any physical barriers that have been provided to determine how movement is facilitated, where technologies are located and access restrictions to sensitive networks and infrastructure. Architecture and planning also recognises the various user groups within the facility and how these groups are segregated yet, where applicable, have the ability to interact.   Architecture and planning also give consideration to the principles and philosophies associated with the study of "Crime Prevention Through Environmental Design" (CPTED) being: -

- Natural Surveillance

- Natural Access Control, and

- Territorial Reinforcement

CPTED considers internal and external environment features such as:

- Building setbacks

- Landscaping (including and excluding trees and shrubbery)

- Streets/footpaths

- Public areas

- Parking lots and structures

- Reception areas

- Corridors

- Receipt and dispatch areas

- Foyers

2.3. Technology

The technology element of security refers to the equipment and systems that are provided to assist security management in obtaining the level of security necessary to meet the identified risks. Management, Architecture & Planning and Technology, must be considered to ensure they are compatible with the intended function of the ROC. The aim of security management is to ensure the maximum utility of any facility subject to that facilities security requirement. Further, it is important to note that technology must not be used simply because it exists. Proposed technologies must be carefully investigated and selected to compliment the intended function of the facility, the defined management procedures and the architectural design of both the existing building and the fit out of the ROC.

The synergistic combination of management, architecture with planning, and technology must deliver a balanced security solution and therefore a level of security transparency.

3. Purpose of the VeriSign Australia Security Policy

The VeriSign Australia Security Policy is a set of security objectives that guide how the assets (i.e. equipment, services, information and personnel) are managed, protected and distributed.

The ultimate objective of this security policy is to create a framework through which, when properly implemented, ensures VeriSign Australia achieves the highest possible level of security. In this manner we have considered both the real and perceived risks to the business and successfully developed a totally secure environment.

This security policy addresses the entire system upon which the Certification Authority is based, and implements procedures that successfully deliver the provision of Public Key Infrastructure and Digital Certificate Issuance.

These policy statements are in accordance with recognised international PKI and GateKeeper standards.

4. Standards

The VeriSign Australia Security Policy is based upon the following standards:

- o ACSI (Australian Computer Security Instructions) 33 "Security Guidelines for Australian Government IT Systems April 1998. http://www.dsd.gov.au/infosec/acsi33/cover.html

- o ACSI 37 – Australian Government Standards for the Protection of Information Technology Systems Processing Non-National Security Information at the Highly Protected Classification.

- o ACSI 37 Supplement – Certification Test Procedures for Information Systems Processing Highly Protected Data.

- o Commonwealth Government Protective Security Manual.

- o GateKeeper – "A strategy for public key technology use in the Government". OGO - Gatekeeper - Index page

- o Information Security Management - Specification for Information Security Management Systems AS/NZS 4444.2 (7799)

5. Roles and Responsibilities

5.1.   Chief Technology Officer

The Chief Technology Officer is responsible for the:

- Operational Management of the entire Certification Authority.

- Preparation, publication and communication of VeriSign Australia's internal policies and procedures.

5.2.   Security Manager

The Security Manager shall be responsible for the day-to-day administration of Information Security within VeriSign Australia together with:

- Development and implementation of physical security procedures and policy.

- Development and implementation of IT Security procedures and policy.

- Administration and supervision of the change control process.

- Monitoring of audit trails.

- Provisioning of IT Security awareness through VeriSign Australia.

- Detection of Security violations or compromises.

- Education of all users regarding security policy.

- Enforcement of policy throughout the company.

- Management of the Critical Incident Response Team (CIRT).

- Escalation and notification of incidents to senior management.

All operational personnel are responsible for ensuring compliance with VeriSign Australia's suite of security policies.

5.3.   Facility Access Administration

Responsibility for the administration and maintenance of all security access controls to the VeriSign Australia ROC lies with the Security Manager.

Alterations to personnel access profiles shall be made in a timely manner so as to accurately reflect staff additions, terminations and movement.

6. Publication

Good management practice and GateKeeper Accreditation criteria insist on the production and implementation of various security policies and plans. In accordance with these criteria, VeriSign Australia has prepared a policy titled '***Security Policy – Public'*** that is publicly available at the following URL:

http://www.verisign.com.au/repository

7. Legislation

Through the Security Policy, Information Systems Security Plan (ISSP) and the Physical Security Plan, VeriSign Australia shall meet all legal obligations in respect of the protection of data, including the confidentiality of that data as required by the following Acts, Regulations, Policies and Standards.

- VeriSign Australia Policies and Procedures.

- Privacy Act 1988, Section 14.

- Commonwealth Crimes Act 1914, Sections 70 (1), (2) and Section 79.

- Copyright Act 1968

- Freedom of Information Act.

- Archive Act 1983.

- The Protective Security Manual.

- Data Protection Bill (Vic).

- National Principles for the Fair Handling of Personal Information February 1998.

This legislation applies to all electronically stored information.

8. Trusted Employees

As part of the high standards of trust and security implemented by VeriSign Australia, all employees must submit to background financial and criminal checks to help establish their ability to maintain the required high level of trust.

This requirement is detailed in full in the VeriSign Australia 'Trusted Employee Policy'.

As detailed in this policy all employees are required to obtain clearance at one, if not two, levels of vetting dependant upon their respective role and duties.

The first level of vetting involves:

- Criminal history check with the Federal Police,

- Insolvency check with the Insolvency Trustee Society of Australia,

- Character checking through five nominated referees, and

- Identification confirmation through photographic id.

The second level of vetting consists of clearance through the Australian Security Vetting Service (ASVS) to the security clearance level of 'Highly Protected'

This level of vetting relates to employees performing any of the following duties:

- All GateKeeper associated functions including financial/project/account related roles.

- Any employee interacting with Government clients,

- All employees working within the secure 'Processing Centre'

- Positions of extreme trust such as Security Manager and Cryptographic Key Manager

- All staff having high levels of logical network access.

9.   Disaster Recovery Plan

It is the responsibility of Operations Manager to ensure that effective and up to date Disaster Recovery Plans are maintained at all times.   Such plans shall be tested and reviewed on a regular basis under the direction of the Technology Director or his delegate.

For each system, the Engineering Services Manager will be responsible for ensuring that:

- Security risks are identified and the Security Manager informed so that re-evaluation of the Threat and Risk Assessment can be done.

- Personnel that they are responsible for are trained on a regular basis in the appropriate contingency procedures.

- Backup procedures are sufficiently accurate, detailed and timely to provide for recovery purposes.

- Procedures exist for the transition back to normal operations after any disaster or critical incident.

The Executive Manager – Operations is responsible for ensuring that a Disaster Recovery Plan is established which includes:

- Pre-disaster procedures for backup and archiving sufficient for restoration of the facilities and any critical applications.

- Guidelines for evaluating emergency situations and the determination of emergency requirements.

- The establishment of a 'Critical Incident Response Team'.

- Contingencies for the provision of interim facilities, movement to those interim facilities and the return to normal operational activity.

- Procedures for data and software backup and recovery.

- Procedures for the testing of contingency arrangements.

All staff that would be affected by a disaster or critical incident are to be made aware of their responsibilities under the Disaster Recovery Plan and are to be trained on a regular basis for their respective task.

A Disaster Recovery and Business Continuity Plan (DRBCP) has been developed to ensure the timely recovery of processing facilities and databases in the event of a major disaster or failure.   The plan ensures the speedy resumption of essential operations and focus's primarily on keeping critical business processes and services running. This includes staffing and

other non-computing requirements, not merely on the fallback arrangements for computing systems.

DRBCPs are to be tested on a regular basis to ensure that they are effective. Such tests will ensure that the plan is fresh in the minds of all members of the Critical Incident Response team and other relevant staff. A test schedule for the plan will be formulated which indicates how and when each element of the plan is tested.

DRBCPs tend to quickly become out of date due to business changes therefore they will be updated on a bi-annual basis to protect the initial investment in developing the plan and ensuring its continuing effectiveness. Examples of changes that might necessitate updating BCP's include:

- Acquisition of new equipment
- Upgrading of existing operational systems;
- Detection and control technology (e.g. fire detection);
- Staff changes;
- Changes of contractors or suppliers;
- Changes of addresses or telephone numbers;
- Termination, modification, or introduction of new business processes;
- Changes in system operating practices; or
- Changes in legislation.

10. Confidentiality

VeriSign Australia processes requests for digital certificates. The information necessary for a certificate request is used to populate a field in an X.509 Certificate. Proof of identity (validation) information collected during the registration process (such as an email address or business registration information) is considered to be of a 'private and confidential' nature. It is the intention of VeriSign Australia to collect sufficient information to prove the identity of a person or company for the purpose of a certificate application and to ensure that the confidentiality of such information is maintained. The amount of proof of identity information asked for will depend on the class of certificate being requested. (i.e. more information is required for a Class 3 request than a Class 1).

Proof of identity information is considered to be confidential information and as such requires strict protection from unauthorised disclosure. Information received 'on-line' is only accessible by select staff with a demonstrated need for access to that information. Proof of identity Information received in personal applications is secured by means of physical separation from other records and maintained under locked control at all times.

All physical proof of identity information held in the possession of VeriSign Australia is stored in Class B security containers that are subject to security provided by the physical and logical security systems of the Processing Centre and strict logical and physical access control.

Private keys generated during the certificate registration process are generated on the computer of the client or applicant. VeriSign Australia has no access to the private key of any individual or company.

A personal identification number (PIN) is emailed to the applicant at the time of registration and this is used through a specified web site to activate the certificate. This registration process results in no information being provided to VeriSign Australia.

11. Firewall Configuration

The configuration of the Firewalls on the VeriSign Australia Production Network is considered to be security sensitive and is therefore classified as 'Highly Protected'. Only the Security Manager, Security Auditors, and Systems Engineers, are to have access to that information.

11.1. Policy Documentation

The following Internal documentation is classified as 'Highly Protected' and is to be secured in a 'B' class security container:

- Threat and Risk Assessment,

- Cryptographic Security Policy,

- Information Systems Security Plan, and

- Physical Security Plan.

11.2. VeriSign Australia CA Private Keys

The confidentiality of the VeriSign Australia Certification Authority private keys is ensured through the following:

- Multi-tiered physical security,

- Complex logical security measures including intrusion detection systems, multiple firewalls and system auditing,

- Strict physical access restrictions,

- Implementation of policy restricting personnel being allowed alone in areas used for Key Generation or Key storage,

- Vetting of personnel,

- Full Disaster Recovery facilities.

12. Network Security

The standards implemented for network security for the VeriSign Australia computer systems are in accordance with the standards outlined in the Defence Signals Directorate (DSD) publication, ACSI 33 "Security Guidelines for Australian Government IT Systems, April, 1998".

13. Integrity

Certificate Requests and certificate information within the CA system and the X.500 directory may not be modified, deleted or amended in any way by operations personnel. This is enforced through the use of strict logical access control combined with regular audit of the VeriSign Australia network.

Only authorised CA and RA operations personnel are permitted to add new Registration Requests to the CA system. Such registration requests entered into the system may not be modified, deleted or amended in any way.

Application level and database level auditing will be implemented to supervise all access to this information.

The database itself is protected by assignation of a username and password.

14. Availability

In accordance with the VeriSign Australia Service Agreement, the X.500 directory is available to clients at all times.   The inability of clients to access this database means that certificate requests cannot be processed until the resumption of service.   This in turn has the effect that an end user may not be able to use their client PKI application or to rely on a certificate.   It is therefore imperative that VeriSign Australia maintains the ability for clients to access this service at all times.

The Certificate Revocation List (CRL) is to be available at all times to ensure that customers have the ability to verify a certificate they are dealing with has not been revoked for any reason.   The inability of a customer to perform this check against the CRL could result in transactions occurring that would not normally have been made, were the CRL available.

15. System Documentation

Access to internal policy and procedural documents including the Information Systems Security Policy, Physical Security Plan, Threat and Risk Assessment, Certification Authority Operating Procedures and Registration Authority Operating Procedures is restricted to the following personnel:

- Managing Director

- Executive Manager – Operations

- Security and Operations Manager

- Engineering Manager

- Lead Engineers

- Software Development staff

- Technical Document Writers, and

- Security Auditors

All documentation published on the VeriSign Australia website is protected from alteration, deletion or damage by unauthorised persons by the implementation of firewalls and intrusion detection systems.

16. Protection of Keys

It is absolutely imperative to protect the signing keys of VeriSign Australia's trusted system and ensure that there is no possibility of compromise. Disaster Recovery, Threat and Risk Assessment and Business Continuity Plans have all been developed to guarantee the security, availability and integrity of the signing keys.

The following signing keys form the basis of the VeriSign Australia trust network:

- eSign Australia Gatekeeper Root CA

- VeriSign Australia Class 2 OnSite Individual Subscriber CA

- VeriSign Australia Class 3 OnSite Enterprise Administrator CA

- VeriSign Australia Class 3 OnSite Operational Administrator CA

- VeriSign Australia Class 2 CA

- Imperito Root CA.

17. Physical Security

The VeriSign Australia Regional Operations Centre (ROC) is a secure facility that has multi-tiered physical security barriers. Based on the military principle of 'defence in depth', each layer of the security builds upon the previous layer ensuring that the innermost areas are controlled by strict multi-layered security controls.

The security technology utilised in the ROC comprises an integrated solution of the latest and most appropriate technologies available to satisfy the individual requirements that each component must perform.

Each of the technologies is of the latest generation in software (i.e. that the software platform, whilst proven, has been developed in recent times). Wherever possible this philosophy has been maintained, however it should be noted that the design specifically incorporates SCEC endorsed Type 1 Security Alarm System componentry.

18. Physical Asset Recording

All physical hardware assets including computer equipment, furniture and computer software is recorded in an 'Assets Register'. This register is maintained by the Operations Manager and is updated on the following occasions:

- Addition/ Removal/ Alteration of equipment

- Existing asset is no longer serviceable due to

    o Damage,

    o Age

    o Change in technology

- Transfer of equipment to a different company location

- Upgrade of existing asset

All assets are labelled with a unique identification bar code label, the details of which are recorded on the asset register together with a full description of the item itself.

19. Critical Incident Response

The Technology Director has formed a Critical Incident Response Team (CIRT) to effectively respond to critical incidents affecting VeriSign Australia and to implement the disaster recovery plan. The team consists of the Engineering Services Manager, Operations Manager, Security Manager and any others deemed necessary to effectively respond to any incident.

The aim of the team is to:

- Determine access point to the resources,

- Document occurrence,

- Minimise the effect of any incident on VeriSign Australia business practices,

- Implement strategies for harm minimisation,

- Dynamically respond to the incident in 'real time',

- Gather available evidence for disciplinary or court proceedings, and

- Notify Senior Management.

Certain incidents require a tactical decision to be made at some stage as to cessation of the activity that constitutes the incident, i.e. what point to 'boot' a person attempting to penetrate firewalls etc. This decision is to be made by the Technology Director or his nominee at the time of any incident bearing in mind the following considerations:

- Absolute priority is the minimisation of risk or threat to VeriSign Australia systems,

- Identification of any weakness in system,

- Identification of any person involved, and

- Significance of evidence gathered.

A written record is compiled by the Security and Operations Manager for all 'Critical Incidents' that take place. This documentation is reviewed by the Technology Director and maintained on hand and available for audit purposes.

20. Internal Breach of Network

In the case of an internal breach of IT security by an employee, the Engineering Services Manager is to be notified and management informed through the Security Manager.

A number of choices are available to management in such instances:

- A formal meeting with the employee and dismissal or official warning action can be taken. This will be dependent on the past history of the employee and the severity of the breach.

- In the case of industrial espionage, the matter can either be pursued civilly or criminally. This will have to be decided at the time as the evidence required for either avenue differs substantially. Advice is to be sought from relevant law enforcement agencies i.e.: Victoria Police Computer Crime Investigation Squad or Federal Police Computer Crime Squad if criminal proceedings are to be considered.

All relevant logs may be required as evidence in any future court proceeding. Therefore they must be correctly marked/labelled and stored in a secure location.

If civil action is to be taken by VeriSign Australia against a member of staff, legal opinion is to be sought.

21. Internal Breach of Network

In the case of an internal breach of IT security by an employee, the Engineering Services Manager is to be notified and management informed through the Security Manager.

A number of choices are available to management in such instances:

- A formal meeting with the employee and dismissal or official warning action can be taken. This will be dependent on the past history of the employee and the severity of the breach.

- In the case of industrial espionage, the matter can either be pursued civilly or criminally. This will have to be decided at the time as the evidence required for either avenue differs substantially. Advice is to be sought from relevant law enforcement agencies i.e.: Victoria Police Computer Crime Investigation Squad or Federal Police Computer Crime Squad if criminal proceedings are to be considered.

All relevant logs may be required as evidence in any future court proceeding. Therefore they must be correctly marked/labelled and stored in a secure location.

If civil action is to be taken by VeriSign Australia against a member of staff, legal opinion is to be sought Purpose

22. External Breach of Network

In the case of an external breach of either VeriSign Australia computer network, the first priority is to stop the breach itself. If an individual is attempting to gain access to the network, all efforts must be made to stop successful access being made. If the access is successful, then the Critical Incident Response Plan is to be implemented.

All server log files are to be maintained and stored in a secure area. In this instance the backed up logs are important as this will assist with isolating the first access or any numerous accesses made.

23. Reporting Procedure – External or Internal Breach

In the case of any internal or external security breach, the following procedure is to be followed:

- The Security Manager & Engineering Services Manager are to be notified so the proper response can be implemented.

- The Technology Director is to be notified immediately and fully briefed as to the situation.

- The Security Manager and senior management are to decide on the relevant course of action as outlined above.

- A systems administrator is to retrieve and maintain all relevant server log files. In the case of files being changed, they are to be isolated and maintained for further analysis by the relevant authorities. During this process, comprehensive notes are to be made as to all steps undertaken.

- The system is to be restored to its 'original' format.

If any security breach has an affect on any customer whatsoever, the Customer Service Director is to be made aware of the security breach. This is to ensure that Customer Service personnel are in an informed position regarding any incident that is liable to provoke a customer response.

24. Dual Occupancy Zones

VeriSign Australia has implemented 'dual occupancy' zones within specific areas of the eight-tier security facility.   This effectively means that there are areas of the facility where no person is ever permitted to be alone and 'dual occupancy' is required whenever these areas need to be accessed.

The VeriSign Australia 'dual occupancy' zones include:

- Any area used for storage of online cryptographic materials,

- Any area used for storage of offline cryptographic materials,

- Key Ceremony Room when a ceremony is being conducted,

- Data Centre housing the Production Network.

25. Employees Responsibilities

All individuals are required to sign a confidentiality agreement upon commencing employment with VeriSign Australia.

All individuals are to read and sign an acknowledgement confirming they have read and are prepared to comply with the VeriSign Australia Employee Handbook.

All employees authorised to use computer resources are responsible for all use of their logon access and must keep their passwords confidential to protect VeriSign Australia computer resources.

Any individual who uses wide-area network services such as the Internet, provided via the VeriSign Australia infrastructure is to abide by the rules detailed within the VeriSign Australia Employee Handbook.

No employee shall attempt to access VeriSign Australia resources for which they have no authorisation.

Employees are responsible for;

- Following procedures, including safeguarding passwords and avoiding the risk of computer viruses.

- Reporting security violations or attempted security violations to the Security Manager or the Engineering Services Manager.

- Reporting instances of actual or suspected computer virus infections to the computer security officer or systems administrator.

- The following of local procedures governing the security of information

- Protecting information appropriately, including that which is at an early stage of preparation or discussion and may not yet be formally recorded on an information system.

- Securely transmitting information in a manner that minimises the risk of accidental or deliberate misuse outside VeriSign Australia.

26. Access Control

26.1. Passwords

Access control to the VeriSign Australia computer networks is governed by password and/or digital certificate control. All personnel are required to adhere to guidelines in respect of password composition, use, longevity and security as per the Employee Handbook.

A regular audit is conducted on passwords in use on the system to ensure that they all comply with VeriSign Australia guidelines.

26.2. Electronic Mail

Electronic mail facilities are provided for employees to assist them in the day-to-day execution of their duties. If such facilities are used for the transmission of personal messages, they shall be treated no differently then work related messages. VeriSign Australia reserves the right to access any personal mail and to copy or delete such mail as required and to disclose the messages to any party deemed appropriate.

Personal use must not:

- Interfere with normal business activities,

- Involve any form of solicitation,

- Be associated with any outside profit oriented business activity,

- Be used for the exercise of the users right to free speech,

- Be used for any activity that could potentially embarrass VeriSign Australia,

- Involve the distribution or otherwise handling of offensive or pornographic material, and

- Involve misrepresentation, obscuring, suppression or replacement of another person's identity.

The receipt of any e-mail that is found to be offensive, anonymous or appears to have been written by someone other than the apparent sender, is to be reported to the Security Manager. The e-mail is not to be deleted unless instructed by the Security Manager.

Any abuse or misuse of email facilities or privileges is unethical, unacceptable and is just cause for invoking sanctions or other disciplinary action.

27. Computer Viruses

It is the responsibility of the Engineering Services Manager to ensure that:

- Virus protection is installed on all servers and computers operating on all VeriSign Australia networks.

- Current virus updates are to be obtained and installed on all computers and network servers. This is to be done immediately they become available.

All external media entering the site is to be scanned for viruses by the Security Manager before being used.

All users must immediately notify Technical Services and the Security Manager whenever they believe a virus or other harmful program has been detected. This will ensure that proper procedure can be followed to prevent further infection and ensure the eradication of the virus.

28. Network Infrastructure Security

The VeriSign Australia Production Network and Corporate Network are designed using a combination of firewalls, high availability firewall software and intrusion detection systems to provide a secure networking environment. With a dedicated Network Management System, real time monitoring of the entire network infrastructure occurs providing instantaneous alerts to system administration personnel.

In addition to this a paging system has been established to provide for real time alert notification in the event of any incident-taking place on the network.

29. Data Security

The owner of information shall be responsible for ensuring that any data under their control is classified appropriately according to its sensitivity, confidentiality and criticality.

All classified material is to be protected in accordance with the guidelines publicised in the VeriSign Australia Employee Handbook.

30. Sensitive Media Marking and Storage

When sensitive information is written to a floppy disk, magnetic tape, smart card, CD-ROMs or other storage media, the media is to be suitably marked with the highest relevant sensitivity classification. When not in use all media with a 'Highly Protected' classification is to be stored in class B security containers.

31. Media Security

The term "IT storage media" refers to magnetic tape cartridges, computer hard disk drives, removable diskettes, CD ROMs, DVD and other disk storage equipment.

System Administrators are responsible for ensuring that when IT storage media is reused or disposed of, there is no possibility of a breach of confidentiality through unauthorised access to any residual data or information on the media.

IT Storage media shall be disposed of in accordance with the Protective Security Manual and according to the highest classification of data it has ever contained and the degree of risk associated with a breach of data confidentiality.

Media that has been used for the storage of 'Highly Protected' information is not to be re-used for the storage of information of a lesser security classification.

The Security Manager is responsible for securing IT storage media pending disposal in a Class B Security Container in accordance with provisions of Part VI of the Protective Security Manual.

32. Data Transfer and Storage

Any IT storage media used to transfer information is not to contain residual information that 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.   Storage media that has previously contained highly classified information or data remains rated at the security classification of that data.

33. Portable/Laptop Computers

The responsibility for the protection of VeriSign Australia portable computers and the data contained thereon resides with the person to whom the equipment has been provided.

When used to process sensitive data such as 'Confidential' or 'Commercial in Confidence' the portable computer shall be configured to require a password to be entered during the boot up process.

All sensitive data stored on laptop/portable computer hard disk drives is encrypted through an automatic encryption process that is enabled as part of the Standard Operating Environment.

Laptop/portable computers are loaded with an approved virus scanning program which is to be kept up to date at all times.

Portable/laptop computers are to be kept in a secure place at all times when not in use or unattended for any length of time.

Portable/laptop computers are not to be left in an unattended motorcar unless in extreme circumstances. In any such case they are to be placed out of sight, preferably in the boot and the vehicle is to be securely locked.

34. Privately Owned Computers or Software

Privately owned equipment is not to be connected to VeriSign Australia computer systems. There is to be no exception to this rule.

Portable computers used by Contractors are not to be connected to the Production Network. Prior to any connection to the Corporate Network they are to be examined to ensure that up to date virus software is installed.

The use of privately owned removable media in connection with VeriSign Australia computer systems is forbidden.

All VeriSign Australia computers are configured to a Standardised Operating Environment. The alteration of this environment by the addition of software is to be approved by the Security Manager.

35. Configuration Management

Configuration Management control has been implemented to ensure that changes not only introduce the desired effect but result in the systems continued ability to process ongoing business demands. One such demand is security, therefore Change Management Control always ensures that any proposed changes to the baseline configuration, do not degrade the system security in any way. All changes to the baseline configuration necessitate re-evaluation of the Threat and Risk Assessment to determine any change in the threats applicable to the business.

Configuration Management Control will be followed to monitor all changes to the baseline configuration to computers on all VeriSign Australia networks including:

- Hardware changes,

- Software changes,

- Documentation for either of the above.

A fully documented baseline configuration has been established for VeriSign Australia. This baseline configuration or Standardised Operating Environment (S.O.E) is upgraded uniformly throughout VeriSign Australia as needed.

The Technology Director shall approve any changes to the SOE.

Any change to the baseline configuration whether it is software, hardware or documentation changes, must be recorded by the change control mechanism.

36. Change Management Control Board

A Change Management Control Board has been formed as part of the formal management process. The board constitutes representatives from:

- Security,

- Engineering Services,

- Customer Service, and

- Operations.

The Change Management Control Board must consider every change in hardware, firmware, software or procedures, and the affect of any change on the security and availability of the network.   Once approval for a change has been determined, the requested change is to be forwarded to senior management for final authorisation.

Changes are not to be implemented until they have been authorised by senior management.

37. Software Control

Software control includes software selection, installation, development and documentation. The Change Management Control Board governs all operational software used by VeriSign Australia. The only exception to this is software programs being used for research purposes, which can only be used in an evaluation environment, separate to any production or corporate networks.

38. Privacy

Safeguarding the privacy of personal information is the responsibility of all employees of VeriSign Australia. It is important for every employee to respect the privacy of others.

Where access rights and privileges will result in access to and use of personal information held by the company in computerised formats, access will only be granted where there is a demonstrated need for this in terms of an employee's duties.

During audits it will be necessary for the Security Manager to access email stored on or transmitted via VeriSign Australia's facilities for security monitoring purposes.

Access to other user files, unless directly related to work purposes, is to be avoided. Employees, who access any part of the network without the appropriate authority, leave themselves vulnerable to criminal or civil proceedings.

No employee is to access or disclose personal or private information, except in strictly limited circumstances. These circumstances include but are not limited to the following;

- With the consent of the person to whom the information relates.

- Under statutory authority.

- Pursuant to some other legal obligation.

In all these cases, such release of information will be under the supervision and approval of the Technology Director.

39. Operations

VeriSign Australia has established a PKI Certification Authority that meets the Gatekeeper Accreditation standards.

Subordinate entities to the Certification Authority shall conform to all VeriSign Australia PKI requirements.

Key and certificate transport mechanisms ensure that only lawful owners receive private keys and their associated certificates and authorised users receive public keys.

A X.500 directory is provided and maintained to facilitate access to certificate status and public keys.

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

- Concept of Operations

- Threat and Risk Assessment

- Information Systems Security Plan

- Disaster Recovery Plan

40. Technology

The Root Certification Authorities, Certification Authorities and Registration Authorities subordinate to the VeriSign Australia hierarchy have achieved Certification of underlying technology elements to Common Criteria EAL4, in accordance with:

- Gatekeeper Accreditation requirements;

- Section 23 of ASCI 33 – Multi Level Networks - Non-National Security Classified Systems, and the

- VeriSign Australia specified security target.

The VeriSign Australia PKI shall operate under the general auspices of the Security Guidelines for Australian Government IT Systems (ACSI) 33 and 37, the Protective Security Manual (PSM) and the standards document AS/NZS 4444, which cover the following topics:

- Preparation;

- The Environment;

- Technical Security;

- Security Audit and Review;

- Network Specific Considerations;

- Small Systems Security;

- Miscellaneous Topics.

No member of VeriSign Australia staff is to:

- Use any VeriSign Australia computer or network facilities without proper authorisation or for unauthorised purposes;

- Assist in, encourage, or conceal any unauthorised use, or attempt at unauthorised use, of any of the computers or network facilities.

- Knowingly endanger the security of any VeriSign Australia service computers or network facilities, nor wilfully interfere with others' authorised use.

41. Software Copyright

Copyright laws limit the ways in which software and data can be used. Any breach of copyright can result in litigation against both the user and the company. All VeriSign Australia staff are to ensure that copyrighted software and associated material is used in accordance with the terms of the relevant licenses. Only authorised software is to be used by all personnel. This means software that has been legally obtained or developed, and is used in accordance with any applicable conditions of acquisition.

System administrators must ensure that mechanisms are implemented and maintained that verify only authorised software is being used. Such checks and procedures will be performed on a frequent basis. Any unauthorised software detected on the network is to be brought to the attention of the Security Manager immediately.

The Security Manager is to ensure that all users are adequately advised of the requirements of this copyright policy, and the proper procedures that are to be followed.

42. Sanctions

Where an authorised user has been found to misuse the resources to which they have been granted access and/or has performed activities prejudicial to the security of those resources, such action must be documented and referred on to the Security Manager who is to notify senior management.

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

Depending on the nature of the users actions, sanctions may range from counselling or suspension of system access rights through to dismissal and/or legal action. Where the nature of the users actions forms part of a period of improper behaviour or poor work performance, process will be taken to ensure the employee is warned regarding their performance.

43. Education and Training

Training in security matters is an essential element in providing staff and contractors with the skills and knowledge necessary to meet their responsibilities. Training for all staff is to be conducted on a frequent basis to ensure that all personnel are aware of their obligations and to educate them as to their responsibilities regarding security.

It is the responsibility of the Security Manager to ensure the provision of ongoing training in security throughout VeriSign Australia.

This training includes the introduction of all new members of staff to the Security Policy and full explanation of all responsibilities.

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