Global Information Assurance Certification Paper

Implementing ISO/IEC 17799 Within a HIGHLY-PROTECTED Environment

by

David Begg GCIA

GIAC Certified ISO-17799 Specialist Practical Assignment

Version 1.0, December 2003

Challenge

20 July 2004

Contents

Part 1 Define the System

1.1 The Organisation

The organisation involved in this ISMS project is a government agency with approximately 140 staff. The organisation is located on several floors in one building. The primary functions of the organisation are:

- Dealing with complaints;
- Oversighting the investigations of complaints;
- Reviewing the implementation of legislation;
- Reviewing the delivery of services;
- Auditing complaint handling systems.

The primary role of the organisation is to serve as an independent review body in the areas of:

- Dealing with complaints against agencies;
- Compliance with law;
- Standards of service provisions;
- Implementation of legislation.

Since the main work of the organisation is in dealing with complaints lodged by third parties and reviewing the operation of other agencies, the organisation mostly holds information that it has gathered from external sources and can easily be acquired again from those sources. Essentially, the organisation possesses very little original information.

A considerable amount of the information that the organisation possesses and accesses is rated by the NSW Office of Information and Communications Technology (OICT) as HIGHLY-PROTECTED according to its "Guide to Labelling Sensitive Information" [6] This guideline defines HIGHLY-PROTECTED information as:

"Information whose compromise could cause serious damage to NSW, the

Government, commercial entities or members of the public eg

- Threaten life directly;
- Seriously prejudice public order;
- Substantially damage state or national finances or economic and commercial interests. "

This OICT guideline in turn refers to the Australian Defence Signals Directorate's (DSD) ACSII 33 Manual [5] for directions on securing HIGHLY-PROTECTED information.

Figure 1 shows the organisational structure. The positions that are shaded make up the Security Committee.

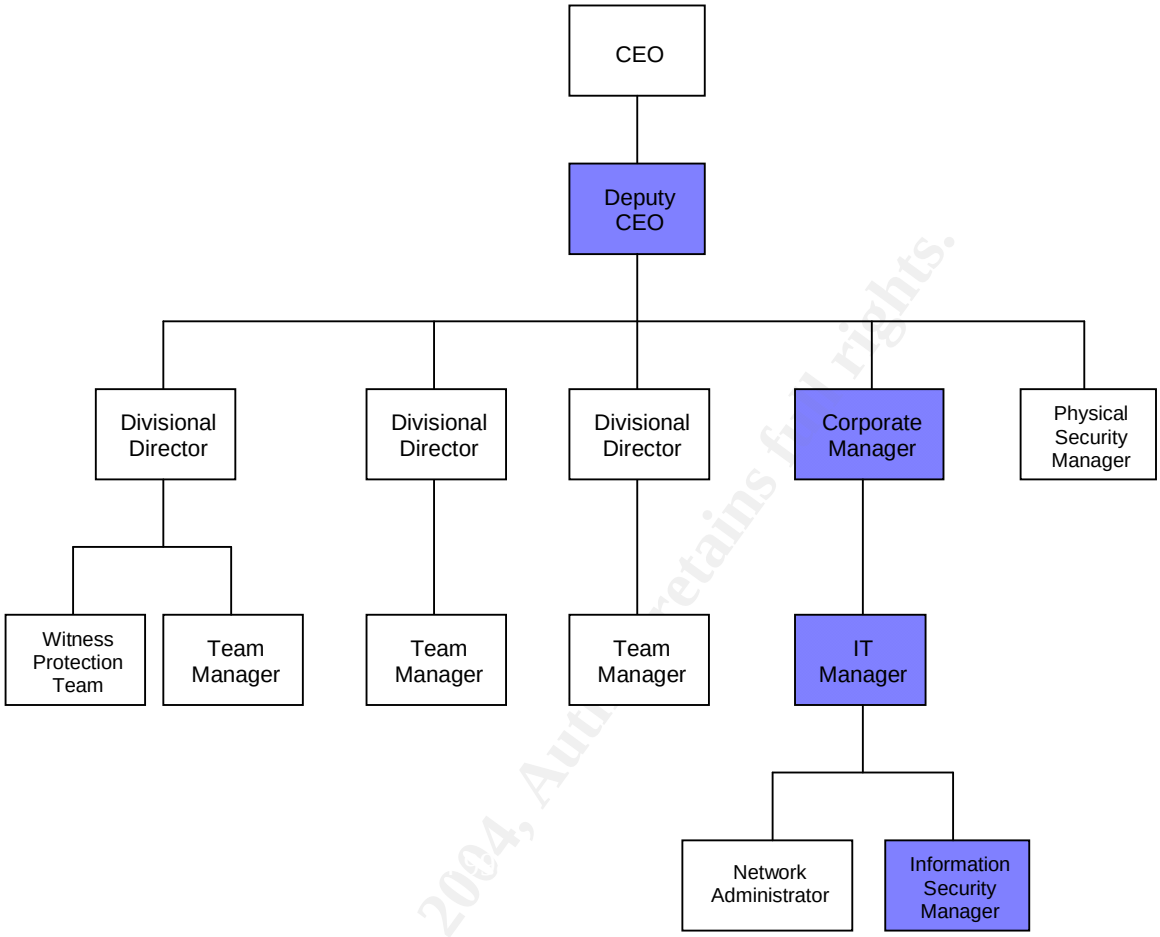

Figure 1: Organisational Structure

1.2 System Description

The ISMS was developed for the systems described in the following sections.

1.2.1 Electronic Document Management System

Currently, an Electronic Document Management System (EDMS) is being implemented and all divisions within the organisation will eventually use it. It will store all electronic documents and will interface with the complaints management systems described in Sections 1.2.10 and 1.2.10. It will become an essential tool since all electronic documents the organisation possesses will be stored within this system.

In the future the EDMS may be extended to record the existence and location of paper based documents, using a bar-coding system.

1.2.2 Email

Email is one of the key methods that members of the public can use to submit complaints to the organisation. It is also an essential means of communication with other agencies.

1.2.3 Floor Access System

The organisation's floor access system is part of the overall building access control system. However, the organisation manages its own portion of the system.

Some complainants that visit the organisation's premises can create a disturbance and on occasion become violent. Consequently, the safety of staff was a serious consideration. The staff who are most at risk are reception staff and enquiries staff who meet personally with the complainants.

1.2.4 Telephone System

The telephone system is the most common means for our customers to contact us to register their complaints and ask for advice. The organisation would be severely restricted in its ability to perform its functions if the telephone system were not available.

1.2.5 IT Services / Helpdesk

IT Services and the Help Desk comprise of three staff, including the IT Manager, the Network Administrator and the Helpdesk Manager. The Helpdesk utilises a helpdesk application for managing service calls.

Because the organisation has become so dependant on it's IT&T systems, the IT Services and the Help Desk are essential functions of the organisation.

1.2.6 Payroll

The organisation has a legal responsibility to pay staff on a regular basis. A HR application is used to manage payments and a dial-up connection to a financial institution is used to initiate payments to staff.

1.2.7 Witness Protection

The organisation runs a witness protection scheme. The data maintained by this function is extremely sensitive, with potentially life-threatening consequences if exposed.

The Witness Protection personnel work in a secure room with a biometric reader for access control. Only authorised personnel have access to the room. The sensitive information that they possess is stored on diskette and kept in a safe within the secure room.

1.2.8 Finance

An accounts package is used to handle the organisation's finances. The organisation has an obligation to pay its bills in a timely manner.

1.2.9 Personnel

Personnel information regarding staff is kept and privacy needs to be maintained. Some personal information is stored in the HR application, which is only accessible by authorised HR staff. Other information is stored in folders on a file server with access controls limiting access to authorised HR staff.

1.2.10 General Complaints Management System

This is an off the shelf complaints management system that is used by all divisions of the organisation. It is an essential tool for managing complaints.

1.2.11 Specialised Complaints Management System

This is a purpose built complaints management system primarily used by one of the organisation's divisions. It interfaces with the general complaints management system and the EDMS. It is a distributed, web based application partially hosted by this organisation and partially hosted by another government agency. Access to the application is across a private, secure WAN used by only a small number of organisations. The information housed by this distributed application is of a very sensitive nature.

1.3 Current State of Security

The organisation has recently made great progress in improving security, based primarily on our participation in the WAN described in section 1.2.11. This has been a high profile project within the organisation and has raised the awareness of security amongst all staff, especially amongst those using this complaints management system.

These security controls have mostly been limited to the network infrastructure. Because the organisation possesses information classified as HIGHLY-PROTECTETD, network security had to be built to the standards defined in the DSD's ACSII 33 Manual [5]. This requires that a HIGHLY-PROTECTED network must be protected from an untrusted network by two EAL4 rated firewalls from different vendors and running on different platforms. Consequently, the organisation is protected from both the Internet and the private WAN by two firewalls. Another requirement of the ACSII 33 Manual is to implement an Intrusion Detection System, which has been done. The management and monitoring of the security infrastructure has been outsourced.

Whilst the project defined stringent security requirements based upon government standards and guidelines, the organisation has no policies to support these requirements.

Antivirus software runs on all PCs, and at the email gateway. All servers are regularly backed up with backup tapes stored in a fireproof safe in the server room. Access to the server room is via swipe card and is restricted to authorised personnel.

Access to the offices is restricted by swipe card. The Witness Protection staff work in a secure office with access controlled by a biometric scanner and is limited to authorised personnel. Witness Protection information is stored on diskette and kept in a safe within the secure Witness Protection office.

One member of the staff is currently responsible for the physical security of the organisation. Additionally, an Information Security Manager has been appointed and he has been given a significant amount of security training. Overall responsibility for security belongs to the Deputy CEO. He is chairman of a security committee that also includes the Corporate Manager, the Manager, IT and the Information Security Manager.

Whilst we have a number of security policies in place, they not been reviewed for some time and have not been widely distributed amongst staff. The procedures carried out by the IT staff are generally quite secure, however they have not been thoroughly documented. No security awareness training is provided to staff.

Whilst the organisation is separated into three operational divisions, the CEO's desire is to allow the movement of staff between divisions. Consequently, all staff have access to most of the information possessed by the organisation. There is a limited amount of sensitive information that is only accessible by authorised staff.

Part 2 Plan

2.1 Steps Required to Improve the Security System

The first task performed to improve the Security System was to establish the Project Plan shown in Table 1.

Phase	Deliverable	Activities
1	Guiding Principles	Develop a draft set of principles to be used to guide the policy development process based on a review of existing materials, reference to best practice and discussion with key stakeholder groups.
2	Physical Security Review	Undertake a detailed assessment of the physical environment and facilities. Prepare an assessment of measures in place and outline measures required to upgrade to an acceptable standard.
3	Logical Risk Assessment	Plan the conducting of a workshop, including if required issue of security questionnaire. Run Risk Assessment Workshop and document results of workshop to identify key issues to focus on during the remainder of the project.
4	High Level Security Model	Prepare a draft high-level information security framework consistent with 7799 and that supports the required interaction with other government departments and external partners. Review and refine the model as a basis for the development of policies and standards.
5	Policy and Standards	Flowing from the high-level security model developed in Phase 4, develop the policies, protocols and guidelines to implement the framework to meet the requirements of the organisation. Circulate the framework and policies for review and comment and amend as required.
6	Security Awareness and Implementation Guidelines	Develop an Implementation Guide to support the implementation of the Security Model and supporting policies. Develop a Security Awareness Program that can be used to assist staff and stakeholders understand: • The key issues associated with security; • Their role in maintaining security; • How they can apply the Security Model and Policies using the Implementation Guide.

Table 1: Project Plan

2.2 ISMS Management Structure

There was no existing committee whose responsibilities could be extended to accommodate information security so a new Security Committee was formed. The following people were assigned to form the Security Committee for the organisation. They are highlighted in the organisational chart shown in Figure 1. The Security Committee will meet weekly to review the progress of the ISMS implementation and to review any security incidents that have occurred and what can be learned from them.

2.2.1 Deputy CEO (Chair)

The reason for choosing the Deputy CEO as the chair for the committee is that this position is across all divisions of the organisation and holds enough seniority to make decisions on security issues that impact the whole office. The Deputy CEO has been given responsibility for all security issues within the organisation.

The Deputy CEO reports directly to the CEO.

2.2.2 Corporate Manager

The Corporate Manager was included in the committee because this position is neutral to the divisions within the organisation. The Corporate Manager also has responsibility for all IT expenditure.

The Corporate Manager reports directly to the Deputy CEO.

2.2.3 IT Manager

The IT Manager is a member of the Security Committee because this position has responsibility for all IT issues. The IT Manager reports to the Corporate Manager.

2.2.4 Information Security Manager

The Security Manager has been assigned responsibility for the day-to-day management of information security within the organisation. The Information Security Manager reports to the IT Manager.

2.3 Guiding Principles

Using ***confidentiality, integrity*** and ***availability*** as guiding principles, we determined which assets are at risk. The results are shown in Table 2.

Guiding Principle	Risks	Controls
Confidentiality of information	Unauthorised disclosure of information could result in the following risks: • Political embarrassment; • Impact on criminal proceedings; • Loss of life (this risk only applies to Witness Protection information).	• Network security controls; • Access controls on information processing systems; • Physical security of information processing facilities.
Integrity of	Alteration of documents could result	• Computer backup system;

information	in: • Political embarrassment; • Impact on criminal proceedings.	• Network security controls.
Availability of critical information	If information is unavailable or is destroyed it could result in: • Political embarrassment; • Impact on criminal proceedings; • Loss of life (this risk only applies to Witness Protection information).	• Computer backup system; • Network security controls, including firewalls and IDS; • Business Continuity Plan; • Uninterruptible power supply.

Table 2: Guiding Principles

2.4 Physical Security Review

A review was performed of the physical security of the organisation's premises. The review identified the following weaknesses in the physical security of the data centre:

- The perimeter walls do not continue to the under side of the floor slab;
- There is a glass panel on the door. If this glass panel is broken, the door handle could be easily reached and the door be opened.

2.5 Policies Needed

2.5.1 Enterprise Information Security Policy

This is a high level policy addressing all areas of AS/NZS 7799 that are applicable to the organisation. The structure of the policy reflects the sections in the standard. Where necessary, this policy makes reference to lower level policies and procedures to provide more detail.

The deputy CEO has endorsed this Policy and the audience is all staff in the organisation. Each policy statement makes reference to lower level policies and procedures as necessary to provide more specific details. This structure keeps the high level policy to a manageable size and ensures that it will not require frequent changes. Consequently, the deputy CEO only needs to approve changes at the highest level.

Staff will only need to read more detailed policies and procedures for topics that are relevant to their responsibilities. Any changes that need to be made on a regular basis can be made to lower level policies and procedures that do not require senior management approval.

The following controls are addressed sufficiently in the Enterprise Information Security Policy:

- Physical Security;
- Power Supply Protection;
- Outsourcing Contracts;
- Cabling Protection.

The following controls are addressed in the Enterprise Information Security Policy, but also require additional detail from lower level policies and procedures:

- Access control;
- Computer systems backup;
- Network security;
- Change control;
- Password management.

The relevant extracts from the Enterprise Information Security Policy can be found in Appendix B1.

2.5.2 Access Control Policy

The purpose of this policy is to ensure that users are only given access to information that they require to carry out their assigned roles. It also prevents unauthorised users from gaining access to information.

The audience for this policy includes all personnel who are responsible for assigning user rights to the network, or any other information the organisation possesses.

This policy is included in Appendix B2.

2.5.3 Computer Systems Backup and Monitoring Policy

The purpose of this policy is to ensure the correct and secure backup and monitoring of the organisation's computer systems.

The audience for this policy includes all personnel who are responsible for backing up and monitoring any computer system that resides at any of the organisation's facilities, has access to the organisation's network, or stores any information belonging to the organisation.

This policy is included in Appendix B3.

2.5.4 Network Security Policy

The purpose of this policy is to ensure that only authorised and controlled access to the organisation's network is permitted.

The Information Security Manager is responsible for ensuring that appropriate and approved controls are placed between the organisation's network and any external networks.

This policy is included in Appendix B4.

2.5.5 Password Policy

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any of the organisation's facilities, has access to the organisation's network, or stores any non-public information belonging to the organisation.

This policy was based on the "Password Protection Policy" from the SANS Policy Project [7] and is included in Appendix B5.

2.5.6 Business Continuity Plan

The main objective of the Business Continuity Plan (BCP) is to identify possible disasters/emergencies and make plans to respond if such situations occur. This planning will minimise the impact of the disaster, reducing any harm to staff and loss to the organisation.

The BCP documents the procedures by which the organisation will manage significant interruptions/disasters/emergencies, ensuring that essential business operations continue to be provided until such time as normal operations can be restored.

This document outlines the specific strategies that will be adopted to manage a range of common situations that often lead to interruptions to normal operations. In addition, the plan incorporates information about the organisation's technical or business environment that will be required to restore operations in the event that temporary premises, IT or other facilities need to be provided.

This document is primarily designed for senior and other key staff of the organisation to assist them to prepare for and respond to situations that may result in interruption to normal business operations. However, as all staff can be called upon to participate in a recovery team, all staff should be familiar with the contents of this plan.

Note: The Complete Business Continuity Plan is not included within this document for size considerations.

2.5.7 Standard Operating Procedures Manual

The Standard Operating Procedures (SOPS) Manual contains procedures required to support the IT&T infrastructure. It also contains configuration settings for all critical information processing systems.

Because it contains sensitive information regarding the operation and configuration of the organisation's IT&T system, it is only to be made available to IT personnel, as the need exists.

Many of these procedures are directly referenced from either the Enterprise Information Security Policy, or other lower level policies. Some of the areas covered by the SOPS Manual that are relevant to the controls under consideration in this context are:

- Physical security of the data centre;
- Change control procedure for IT&T systems;
- Password guidelines.

Note: Due to the sensitive nature of the information contained in this document, no extracts from it will be presented in this document.

2.6 Asset Identification

A workshop was held with key stakeholders from each division. During this workshop, the information processing systems required to support these critical assets were identified and are listed in Table 3. Assets were classified according to

their sensitivity and owners were identified for each asset. Classification was based on the OICT "Guide to Labelling Sensitive Information" [6].

Information Processing System	Classification	Owner
Electronic Document Management System	HIGHLY PROTECTED	Corporate Manager
Email System	IN-CONFIDENCE	IT Manager
Floor Access System	IN-CONFIDENCE	Corporate Manager
Phone System	IN-CONFIDENCE	IT Manager
IT Services / Help Desk	HIGHLY PROTECTED	IT Manager
Payroll	IN-CONFIDENCE	Corporate Manager
Witness Protection Program	HIGHLY PROTECTED	Divisional Director
Finance System	IN-CONFIDENCE	Corporate Manager
Personnel Records	IN-CONFIDENCE	Corporate Manager
Specialised Complaints Management System	HIGHLY PROTECTED	Team Manager
General Complaints Management System	HIGHLY PROTECTED	Divisional Director

Table 3: Critical Information Processing Systems

2.7 Risk Identification

The next step was to identify the risks that these information processing systems are vulnerable to. The risks are listed below:

- No building access;
- Whole building destroyed;
- IT&T equipment failure;
- Power disruption;
- ISP failure;
- Loss of key staff;
- Other agency disruption;
- Unauthorised intrusion.

2.8 Threat and Risk Assessment

The Threat and Risk Assessment Methodology was based on the Australian Standard for Risk Management, AS 4360 [4]. Figure 2 demonstrates the high level activities that were undertaken.

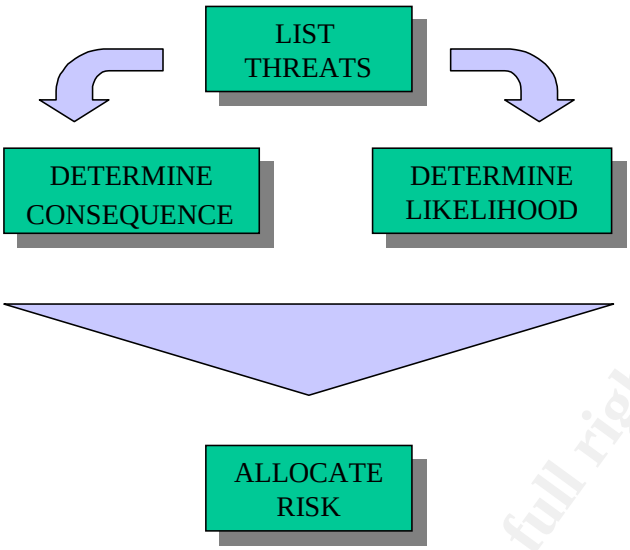

Figure 2: Steps for Determining Risk

The factors used in assessing the risk are:

- **Threats.** Those events that if they eventuate may cause some harm to the Organisation's information assets.
- **Consequence.** This is an assessment of the potential consequence on the Organisation's information assets if a threat was realised. Information assets can include intangible assets such as user community confidence in the Organisation and an inability to carry out mandated tasks in a timely manner.
- **Likelihood.** This is an assessment of the likelihood of each threat being realised (i.e. being successfully exploited), given the existing controls.
- **Risk.** This factor is derived from a calculation based on the consequence and likelihood. It provides an indication of the level of risk inherent with each threat.

The categories of Impact and Likelihood are defined in Table 4 and Table 5. An extract from the Threat and Risk Assessment matrix is shown in Table 6.

Impact		
C	Critical	Extreme impact on the ability of the organisation to continue to function (Less than four hours interruption acceptable)
H	High	Significant impact on the organisation's ability to continue to function (Less than one day's interruption acceptable)
M	Moderate	Moderate impact on the ability to continue to function in the medium term (Less than one week's interruption acceptable)
L	Low	Little immediate impact on the ability of the organisation to function (Less than one month's interruption acceptable)

Table 4: Impact Ratings

Likelihood

C	Almost Certain	Is likely to occur at least once every six months
V	Very Likely	Could be expected to occur once in next the two years
L	Likely	Could be expected to occur once in next the five years
M	Moderately Likely	May occur once in the next twenty years
U	Unlikely	No record of the event ever occurring previously

Table 5: Likelihood Ratings

Risk Matrix for Critical Process			Impact / Likelihood					
			Threats					
Systems of Process	**Responsible**	**Priority**	No Building Access	Whole Building Destroyed	IT&T Equipment Failure	Power Disruption	ISP Failure	Unauthorised Intrusion
Electronic Document Management	Corporate Manager	A	M / M	L / M	C / C	C / C		C / C
Email	IT Manager	A	M / M	M / M	H / C	H / C	H / C	
Floor Access System	Corporate Manager	A	C / M		C / V	M / C		C / M
Phone System	IT Manager	A	M / M	M / M	H / V	H / C		C / M
IT Services / Help Desk	IT Manager	A		M / M	C / C	H / C		M / M
Payroll	Corporate Manager	A	H / M	H / M	H / C	L / C		M / M
Witness Protection	Divisional Director	A	M / M	M / M	M / L	M / M	M / L	C / C
Finance	Corporate Manager	B	M / M	M / M	M / C	M / C		M / M
Personnel Records	Corporate Manager	B	L / M	L / M				L / M
Specialised Complaints System	Team Manager	B	H / M	H / M	H / C	H / C	H / C	H / M
General Complaints System	Divisional Director	B	H / L	C / L	H / V	H / V	M / L	M / L
Risk			**M**	**M**	**C**	**C**	**H**	**H**

C	Critical Risk of Failure or Impact. Less than four hours interruption is acceptable.
H	High Risk – Very Close Attention Required. Functionality must be restored within one week.
M	Significant impact but under control at present. Functionality should be restored within one month.
L	Risk is not significant. Functionality should be restored within one month.

Table 6: Risk Matrix

2.9 Mitigation strategies

The controls shown in Table 7 have been selected as the mitigation strategies required for addressing the four risks that were identified in the TRA as being either Critical or High.

Risk	ISO 17799 Control	Description
IT&T Equipment Failure	8.4.1 – Information backup	The backup tapes need to be stored off-site.
	10.5.1 – Change control procedures	No changes are to be made to critical information processing systems without formal testing and approval.
	11.1.3 – Writing and implementing continuity plans	A business continuity plan needs to be developed to ensure that measures are in place to minimise the likelihood of disruption occurring and to ensure timely recovery when disruption does occur.
Power Disruption	7.2.2 – Power supplies	The existing UPS needs to be upgraded to accommodate all critical IT&T systems.
ISP Failure	4.3.1 – Security requirements in outsourcing contracts	A new ISP is to be chosen to provide a more reliable service and better support.
	7.2.3 – Cabling security	Data connection to the ISP must be protected from damage.
Unauthorised Intrusion	6.2.1 – Information security education and training	All personnel must be trained to be aware of security risks and their responsibilities.
	7.1.2 – Physical entry controls	The weaknesses in the data centre discovered by the physical security review must be addressed.
	8.5.1 – Network controls	A policy must be developed to define what services may be accessed through the network gateways.
	9.1.1 – Access control policy	A policy must be developed to define the access controls that must be implemented.
	9.2.3 – User password management	A policy must be developed to establish password management requirements.
	10.4.1 – Control of operational software	Critical IT&T systems must be patched on a regular basis to protect against security vulnerabilities.

Table 7: Selected Mitigation Strategies

Part 3 Do

3.1 Ensure Computer Backup Tapes are Stored Off-Site

3.1.1 Problem

Whilst backups are taken of all critical computer systems, the tapes are stored in a safe within the data centre. Consequently, if the data centre was to be destroyed, it is likely that the backup tapes would also be destroyed.

3.1.2 Action

The Backup Policy was updated to ensure that tapes are now stored off-site. This control is in accordance with section 8.4.1 in ISO 17799.

3.1.3 Steps

Step One Determine a schedule for moving tapes off-site and returning them to the data centre.

Step Two Update the Computer Systems Backup and Monitoring Policy to include a requirement for storing backup tapes off-site.

Step Three Have the updated policy approved by the owner (the IT Manager).

Step Four Distribute the updated policy to IT&T personnel responsible for performing computer backups.

Step Five Organise a secure off-site storage service for computer backup tapes, using government run service.

3.2 Develop a Change Control Procedure

3.2.1 Problem

No formal process exists for controlling changes to critical information processing systems. The risk is that an unauthorised or untested change could be implemented causing a failure to a critical system.

3.2.2 Action

Develop a procedure for controlling changes to critical information processing systems that reflects the recommendations in ISO 17799 Section 10.5.1.

3.2.3 Steps

Step One Assign authority for approving changes to critical IT&T systems to the IT Manager.

Step Two Agree on a mechanism for gaining approval for changes.

Step Three Develop a procedure for managing changes.

Step Four Develop a Change Control request form.

Step Five Distribute the procedure and form to all relevant personnel.

3.3 Business Continuity Planning

3.3.1 Problem

Whilst a Business Continuity Plan (BCP) was developed for Y2K, it has never been tested. Since this BCP was developed, the organisation has grown considerably, has moved and has undergone significant changes to the IT&T infrastructure. As a result, the existing BCP is completely inadequate for the current needs of the organisation. This means that the organisation has no means of recovering from any serious interruption to its operations and continuing in business.

There is inadequate redundancy in the IT&T system to provide protection against failure of equipment. The risk here is that a failure of any equipment other than hard drives will cause disruption to the operation of critical information processing facilities. Equipment failure could also result in corruption off critical data.

3.3.2 Action

A BCP was developed based on the results of the TRA and as recommended in section 11.1.3 of ISO 17799. Each risk that was identified in the TRA was addressed in the BCP to ensure continuity in the event of a threat being realised. Management chose the controls they wished to implement based on the importance of the process or system affected and the cost of protecting it. For example, one option for business continuity was to establish a redundant site. However, this is an expensive solution that could not be justified.

The BCP has identified the strategies in Table 8.

Division	Business Continuity Strategy
General Business Continuity Strategy	• Defer non-critical activities / tasks until systems are restored • Where possible initiate partial restoration of key systems • Implement alternate business processes including temporary data capture and subsequent data entry to business applications • Temporary relocation of key staff and critical business functions within the office to operable IT systems • Disregard non core functions that depend on the availability of IT systems • Redirect staff to alternate activities until systems restored • Stand down staff who can not be gainfully employed • Implement alternate complaint handling and acknowledgment process • Implement alternate notification handling and monitoring process
Corporate Services Continuity Strategies	• Implement alternate Payroll process • Use CHRIS bureau service • Authorise reuse of previous pay tape • Defer payment of accounts where possible • Raise manual cheque for emergency payments
IT & T Business Recovery Strategy	• Isolate failed system components • Log service calls on failed system components • Purchase / lease replacement systems • Use backup tapes to build temporary systems on available infrastructure • Phased recovery by restoring critical systems first

Division	Business Continuity Strategy
	• Halt low priority applications and divert resources to restoration of key and core business systems • After systems are restored, employ additional staff to complete data entry of data captured on temporary systems into the recovered systems

Table 8: Business Continuity Strategies

3.3.3 Steps

Step One Prioritise the risks identified in the Threat and Risk Assessment.

Step Two Identify potential mitigation strategies for interruptions to the business.

Step Three Select the strategies that are considered appropriate. This will be based on the criticality of the process or system affected and the cost of the strategy.

Step Four Prepare the Business Continuity Plan based on the chosen strategies.

Step Five Assign an owner to the BCP (Deputy CEO).

Step Six Have BCP approved by the Deputy CEO.

Step Seven Distribute the BCP to all personnel who have responsibilities associated with the BCP.

3.4 Improve Data Centre Power Supply

3.4.1 Problem

A power failure in the data centre could cause disruption to the operation of critical information processing facilities and potentially result in data corruption in databases. The building the organisation uses experiences occasional problems with power. Previous electrical contractors have been careless in wiring the building. The result is that some circuits are shared between our organisation and a neighbouring tenancy and the circuits are not clearly documented. At times, electrical contractors working on the neighbouring tenancy have unintentionally interrupted power to our data centre.

A small UPS is currently in place, but is not capable of servicing all of the critical information processing systems in the data centre.

3.4.2 Action

Replace the existing UPS with a larger capacity unit that is capable of supporting the entire data centre and is scalable. It was agreed that the UPS must be able to provide power to the computer systems for at least 25 minutes, to allow time for an orderly shutdown. The UPS must operate at no more than 80% capacity.

The installation of the UPS and the connection of the computer systems to the UPS were done on separate occasions to minimise the risk of problems. Each of these

tasks was performed outside normal business hours to minimise disruption to normal operations.

Configure the UPS and computer equipment so that in the event of an extended power failure, equipment is shut down in an orderly manner.

Employ electrical contractors to document and improve the electrical wiring. This must include ensuring that the data centre is serviced by a unique circuit breaker. Improvements to the electrical wiring were performed outside normal business hours to minimise disruption.

Section 7.2.2 of ISO17799 recommends: “equipment shall be protected from power failures and other electrical anomalies”.

3.4.3 Steps

Step One Calculate the capacity required for a new UPS system.

Step Two Purchase the new UPS system.

Step Three Employ electrical contractors to install and commission the new UPS.

Step Four Employ electrical contractors to audit and document the existing wiring.

Step Five Employ electrical contractors to improve wiring, primarily ensuring that the data centre has its own circuit breaker.

3.5 Select a New ISP

3.5.1 Problem

The organisation relies upon email as a primary source of receiving complaints from the public and for communication with other agencies. Due to our existing ISP experiencing take-overs and mergers, at times it is very difficult to obtain the necessary support when problems with the Internet connection are experienced. Section 4.3.1 of ISO 17799 highlights the need for security requirements in outsourcing contracts to be addressed. Whilst an ISP is not necessarily an outsourcer, the principles still apply since availability of the service is essential to the organisation.

3.5.2 Action

An alternate ISP was chosen with the aim of achieving a more reliable service and better support. The contract with the new ISP included a service level agreement (SLA) dictating the availability of the service. This SLA will be in accordance with ISO 17799 Section 4.3.1.

The configuration changes to computer systems were performed outside normal business hours to minimise disruption.

3.5.3 Steps

Step One Set requirements for new ISP.

Step Two Choose new ISP based on requirements.

Step Three Draw up contract including SLA.

Step Four Migrate DNS records to the new ISP.

Step Five Configure IT&T equipment to use new IP addresses.

3.6 Protect Data Cables

3.6.1 Problem

The organisation relies upon email as a primary source of receiving complaints from the public and for communication with other agencies. If the data cable providing the connection to the ISP were damaged, this could seriously impact on the ability of the organisation to receive complaints and communicate with other agencies.

3.6.2 Action

Develop a procedure to ensure that physical security for data cables are properly protected from damage in accordance with ISO 17799 Section 7.2.3. The risers in public spaces of the building need to be locked and keys only available to authorised personnel.

3.6.3 Steps

Step One Define the controls that need to be implemented.

Step Two Organise with building management to have risers in public spaces of the building locked and keys secured.

Step Three Update the SOPs Manual to include a procedure for protecting data cables.

Step Four Distribute the updated SOPs Manual to relevant IT personnel.

3.7 Develop and Deliver a Security Awareness Training Program

3.7.1 Problem

No security awareness training is currently being provided, either to new staff during the induction process, or to existing staff through an ongoing awareness training program.

3.7.2 Action

All personnel must be kept aware of their responsibilities in regard to the security of the organisations information. This awareness will be maintained by means of a training program in accordance with ISO 17799 6.2.1.

3.7.3 Steps

Step One Develop a program for security awareness training based upon the Information Security Policies that have been developed.

Step Two Develop the training material to be presented, including quizzes to test retention.

Step Three Deliver the training through induction sessions and at regular team meetings.

Step Four Periodically quiz personnel to determine their level of understanding of their security responsibilities.

3.8 Improve Physical Security of the Data Centre

3.8.1 Problem

The physical security review identified that the data centre is accessible by removing ceiling tiles and climbing through the ceiling space over the perimeter wall. Also, the door has a glass panel, which, if smashed, would allow access to the internal handle of the door.

3.8.2 Action

Improve the security of the data centre in accordance with ISO 17799 Section 7.1.2 and the Defence Signals Directorate's ACSII 33 [5].

3.8.3 Steps

Step One Have steel mesh installed in ceiling space above data centre perimeter walls.

Step Two Have steel mesh installed over glass panel in data centre door.

3.9 Develop a Network Security Policy

3.9.1 Problem

With the constant increase in malicious behaviour on the Internet, the risk of experiencing an unauthorised intrusion is ever increasing. Due to the nature of the information the organisation possesses, an intrusion could result in serious political embarrassment, could impact on criminal proceeding and even loss of life.

Although network security is properly implemented at a technical level, there is no policy or mechanism in place to define what services may be accessed through the network perimeter.

3.9.2 Action

Develop a policy describing what services may be accessed through the network perimeter and defining the mechanism for gaining authorisation to make changes to

the services available. This policy will reflect the recommendations in ISO 17799 8.5.1.

3.9.3 Steps

Step One The Security Committee will define the network security controls that need to be in place.

Step Two Draft an information security policy describing the network controls required.

Step Four Finalise the policy with the approval of the Deputy CEO.

Step Five Publish the policy.

Step Six Provide awareness training based on this policy.

3.10 Develop an Access Control Policy

3.10.1 Problem

With the constant increase in malicious behaviour on the Internet, the risk of experiencing an unauthorised intrusion is ever increasing. Due to the nature of the information the organisation possesses, an intrusion could result in serious political embarrassment, could impact on criminal proceeding and even loss of life.

There is no existing policy defining access control.

3.10.2 Action

Develop and implement a policy to define the access controls that are required to mitigate the risk of experiencing an unauthorised intrusion. This policy will take into consideration Sections 9.1.1 of ISO 17799.

3.10.3 Steps

Step One The Security Committee will define the security controls that need to be in place.

Step Two Draft an information security policy describing the access controls required.

Step Three Finalise the policy with the approval of the Deputy CEO.

Step Four Publish the policy.

Step Five Provide awareness training based on this policy.

3.11 Develop a Password Management Policy

3.11.1 Problem

An audit of user passwords has demonstrated that approximately 80% of user passwords could be determined within a few minutes.

3.11.2 Action

Provide users with a policy on selecting secure passwords that comply with ISO 17799 Section 9.2.3.

3.11.3 Steps

Step One The Security Committee will define the quality of passwords that are required to meet security objectives.

Step Two Draft an information security policy describing appropriate password management.

Step Three Finalise the policy with the approval of the Deputy CEO.

Step Four Publish the policy.

Step Five Provide awareness training based on this policy.

Step Six Implement password restrictions within the operating system.

3.12 Develop a Patch Management Procedure

3.12.1 Problem

Currently the organisation has no formal mechanism for ensuring that security patches are applied to critical IT&T equipment in a timely manner. This exposes the organisation as exploits are developed for published vulnerabilities.

3.12.2 Action

Develop a procedure for ensuring that all computer systems, especially critical systems, are patched in a timely manner, as per ISO 17799 Section 10.4.1.

3.12.3 Steps

Step One Determine all critical IT&T equipment that could potentially require patches to be applied to protect against security vulnerabilities.

Step Two Develop a procedure for obtaining approval for and installing security patches.

Step Three Have the procedure approved by the IT Manager.

Step Four Add the procedure to the SOPs Manual.

Step Five Join subscription lists to receive early notification of security alerts.

3.13 Statement of Applicability

The following is an example Statement of Applicability for a control that has been implemented:

ISO 17799 Ref	Policy Ref	Control	Implement	Applicability
9.1.3	9.1.1	Writing and implementing continuity plans	Yes	A Business Continuity Plan has been developed. It outlines the process for the ongoing management of Business Continuity Planning.

The following is an example Statement of Applicability for a control that has not been implemented:

ISO 17799 Ref	Policy Ref	Control	Implement	Applicability
7.4.6	NA	Segregation in networks	No	Because all personnel are allowed access to most of the organisation's information, we don't segregate our network. Any restrictions placed upon sensitive information are implemented by access control systems either at the operating system level, or within the application, according to the Access Control Policy.

Part 4 Check

In accordance with sections 12.2.1 and 12.2.2 of ISO 17799, a process has been put in place to ensure compliance with the security policies and controls is maintained. This section provides the audit checklists required to ensure this compliance.

4.1 Computer Backups Checklist

ISO 17799 Reference: 8.4.1	**Control:** Information backup
Audit Questions	
Are computer backups being performed according to the specified schedule?	
Is the quality of backups checked on a regular basis?	
Are backup tapes stored off-site?	
Importance of the Control	
Reliable backups of critical computer systems are an essential part of the business continuity process. Without backups, there would be no way of restoring the organisation's critical information systems in the event of an emergency.	
Requirements for Compliance	
A backup policy must exist and must be adhered to. Backups must be checked regularly to ensure they can be restored from. Tapes must be stored off-site to prevent them from being destroyed along with the IT&T infrastructure in the event of an emergency.	

Audit Steps	**Findings**	**Compliance**
1. Check to see if the backup policy exists.	A Computer System Backup Policy does exist.	Yes
2. Review logs of the backup server to ensure that computer systems being backed up successfully.	Most backups are successful, however some fail.	No
3. Check that backup tapes are regularly checked that they can successful be restored from. Attempt to restore random data from a recent backup tape.	Tapes are not regularly checked for successful restores.	No
4. Are tapes being stored off-site?	Tapes are being sent of site on a regular schedule.	Yes

This checklist will be used to that backups are successful and that data can successfully be restored from backup tapes.

4.2 Change Control Checklist

ISO 17799 Reference: 10.5.1	**Control:** Change control procedures
Audit Questions	

Does a change control procedure exist?
Is the change control process being followed?
Are changes properly documented?
Importance of the Control
A change control procedure is essential to ensure that changes are not made to critical information processing systems without approval and testing.
Requirements for Compliance
A change control procedure must exist and be followed. Changes must be approved and tested before being implemented. All changes must be documented.

Audit Steps	Findings	Compliance
1. Does a change control procedure exist?	The SOPs Manual contains a change control procedure.	Yes
2. Have change control forms been filled out and approved before changes are implemented?	Change control forms are filled out and retained by the IT Manager.	Yes
3. Are changes tested before being implemented?	Change control forms indicate that testing is performed before implementation.	Yes

4.3 Business Continuity Plan Checklist

ISO 17799 Reference: 11.1.3	**Control:** Writing and Implementing Continuity Plans
Audit Questions	
Does a Business Continuity Plan exist?	
Has the chair of the Security Committee, the Deputy CEO, approved it?	
Has it been distributed to relevant staff?	
Does it reflect the priorities established by management for protecting and restoring information processing systems?	
Have any significant changes occurred to either the business operations or the IT&T system?	
Importance of the Control	
Disruption to critical information processing systems could seriously impact the organisation's ability to perform its functions. A Business Continuity Plan defines mitigation strategies for preventing disruption to systems and business continuity strategies to ensure timely recovery in the event of a disruption. It is essential that the BCP is kept up to date and reflects any changes that occur in either the business operation or the IT&T systems.	
Requirements for Compliance	

The Business Continuity Plan must exist and must be distributed to relevant staff. The BCP must reflect the priorities established by management. The BCP must be stored off-site so it is still available in emergencies. Any staff having responsibilities in regard to business continuity must be trained in the implementation of the BCP. The BCP must be updated when significant changes occur to either the business operations or the IT&T system.

Audit Steps	Findings	Compliance
4. Check to see if the BCP exists and has been approved by the deputy CEO.	BCP Exists and has been approved	Yes
5. Has BCP been distributed to all personnel that have responsibilities defined within it?	An electronic copy of the BCP exists in the electronic document management system	Yes
6. Does the BCP reflect the priorities determined by management for mitigation and continuity strategies?	BCP has addressed the risks that have been identified by the TRA and are properly prioritised	Yes
7. Do all personnel with responsibilities defined within the BCP have hard copies stored at home?	Not all relevant personnel have a copy at home.	No
8. Have relevant personnel been trained in implementing the BCP?	Training has been provided in conjunction with testing of the BCP.	Yes
9. Have any changes been made to business operations that require the BCP be updated?	No changes have taken place.	Yes
10. Have any changes been made to the IT&T system that requires the BCP be updated?	No changes have taken place.	Yes

This checklist will be used to improve the system by ensuring that an up to date BCP exists. It will also ensure that the BCP continues to reflect the priorities set by management.

4.4 Power Supply Checklist

ISO 17799 Reference: 7.2.2	**Control:** Power Supplies
Audit Questions	
Does the UPS have adequate capacity to support the current IT&T system?	
Has the UPS been tested according to the manufacturer's instructions?	
Have all critical computer systems been configured to shut down gracefully in the event of an extended power failure?	
Is the electrical wiring clearly documented?	
Is the data centre serviced by its own circuit breaker?	
Importance of the Control	

A power in the data centre could seriously impact the organisation's ability to perform its functions. It is essential to regularly test the UPS according to manufacturers instructions to ensure that it will perform properly in an emergency situation. Failure to configure computer systems to shutdown gracefully could result in data corruption if a power failure occurs. Properly documented electrical wiring and a dedicated circuit breaker for the data centre will assist in preventing unintentional power disruption.
Requirements for Compliance
The UPS must have sufficient capacity to service the critical computer systems and must be tested according to the manufacturer's instructions. Computer systems must be configured to shut down gracefully in the event of a power failure. Any changes in the electrical wiring must be clearly documented. The data centre must have its own circuit breaker.

Audit Steps	Findings	Compliance
1. Check the load on the UPS is less than 80% as shown on the LCD panel.	Load is 50%.	Yes
2. Check the run time on the UPS is less at least 25 minutes as shown on the LCD panel.	Run time is 30 minutes.	Yes
3. Has the UPS been tested according to the manufacturer's instructions?	Testing has been performed successfully and the results have been recorded.	Yes
4. Have all critical computer systems been configured to shut down gracefully in the event of an extended power failure?	All new systems have been properly configured. Some of the older systems still need to be properly configured.	No
5. Is the electrical wiring clearly documented?	New electrical contractors have been employed and the have accurately documented the wiring.	Yes
6. Is the data centre serviced by its own circuit breaker?	This work has been deferred due to cost.	No

This checklist will be used to ensure that the UPS will be adequate to protect the IT&T systems in the event of a power failure. It will also assist in preventing inadvertent disruption to the data centre power when work is carried out on the neighbouring tenancy.

4.5 ISP SLA Checklist

ISO 17799 Reference: 4.3.1	**Control:** Security Requirements in Outsourcing Contracts
Audit Questions	
Is the ISP meeting the SLA?	
Importance of the Control	

The organisation depends on its Internet connection to complaints from the public and to communicate with other organisations.		
Requirements for Compliance		
The ISP must meet the SLA by maintaining the agreed availability of the Internet connection and providing adequate response to support calls.		
Audit Steps	**Findings**	**Compliance**
1. Review the percentage of availability for the Internet connection during business hours and confirm that it meets the SLA.	The availability does meet the SLA requirements.	Yes
2. Review the response times to support calls and confirm they meet the SLA.	The response times do meet the SLA requirements.	Yes

The Outsourcing Contracts Checklist will ensure that the organisation's ISP meets the SLA. This will mean that complaints can be received via email from the public and that the organisation can communicate electronically with other agencies.

4.6 Cabling Security Checklist

ISO 17799 Reference: 7.2.3	**Control:** Cabling security	
Audit Questions		
Does a policy exist for protecting cables?		
Are cables secured?		
Importance of the Control		
The organisation depends on its Internet connection to complaints from the public and to communicate with other organisations.		
Requirements for Compliance		
A policy must exist describing controls that must be in place to secure cables and it must be implemented.		
Audit Steps	**Findings**	**Compliance**
1. Confirm that a cabling security policy exists.	The cabling security policy statement is contained in the Section 5.2.4 of the Enterprise Information Security Policy.	Yes
2. Is the cable secured according to the policy?	Building risers housing cables in public spaces are locked. Building management keeps the keys and only authorised personnel have access to the keys.	Yes

This checklist will be used to improve the system by ensuring that an up to date BCP exists. It will also ensure that the BCP continues to reflect the priorities set by management.

4.7 Security Awareness Training Checklist

ISO 17799 Reference: 6.2.1	**Control:** Information security education and training	
Audit Questions		
Are all personnel receiving appropriate training in information security to ensure that they are aware of their responsibilities?		
Importance of the Control		
Personnel can only be expected to comply with information security policies if they have been properly trained.		
Requirements for Compliance		
All personnel must receive training and demonstrate understanding of the information security policies.		
Audit Steps	**Findings**	**Compliance**
1. Are policies available to all personnel that need to understand them?	All approved policies have been stored in the electronic document management system and are accessible by all staff.	Yes
2. Have all existing personnel received training in relevant policies?	Regular training sessions are held at team meetings. However, no record is kept of those in attendance.	No
3. Do new employees receive training on information security policies as part of the induction process?	Security awareness training has not been incorporated in induction training.	No
4. Do all personnel understand their security responsibilities?	There is no means of testing understanding of security policies.	No

4.8 Data Centre Physical Security Checklist

ISO 17799 Reference: 7.1.2	**Control:** Physical entry controls
Audit Questions	
Does the physical security of the data centre meet the standard required for the classification of data stored in it?	
Importance of the Control	
Because the organisation possesses information that is classified HIGHLY PROTECTED it is necessary to provide appropriate physical security to the data centre.	

Requirements for Compliance		
The data centre must meet the security requirements of the Defence Signals Directorate's ACSII 33 manual [5].		
Audit Steps	**Findings**	**Compliance**
1. Confirm that the physical security requirements are documented.	Requirements are documented in Section 5.1.4 of the Enterprise Information Security Policy and in the SOPs Manual.	Yes
2. Have the physical security controls been implemented?	Wire mesh has been fitted in ceiling apace above perimeter walls and to the glass panel on the door.	Yes

4.9 Network Security Policy Checklist

ISO 17799 Reference: 8.5.1	**Control:** Network Controls
Audit Questions	
Whether the Network Security Policy exists, management has approved it, owners are responsible for reviewing and maintaining it and it is published to all personnel.	
Whether the policy expresses management's commitment to information security and clearly defines the controls that must be in place.	
Whether a review process exists to ensure that the policy is updated to reflect changes such as significant security incidents, changes to the business process and changes to the IT&T system.	
Importance of the Control	
This policy is an essential part of the defence against unauthorised intrusions into the IT&T systems. Since the organisation possess some information that is classified as HIGHLY PROTECTED, it is essential that it have adequate security, especially from the Internet.	
Requirements for Compliance	
The policy must be available to all personnel. It must be regularly reviewed and updated as necessary.	

Audit Steps	**Findings**	**Compliance**
3. Has the policy been approved by management?	Management have approved the policy.	Yes
4. Does the policy have a designated owner?	The Information Security Manager owns this policy.	Yes
5. Has the policy been reviewed on a regular basis?	The policy has not been reviewed since its implementation.	No
6. Changes are made to the policy as	No changes have been	Yes

necessary.	identified for this policy as yet.	

This checklist is used to ensure that the controls to protect critical information assets are protected against unauthorised intrusions. The policy will be updated in response to significant security incidents and to other significant changes that could open vulnerabilities to the system.

4.10 Access Control Policy Checklist

ISO 17799 Reference: 9.1.1	**Control:** Access control policy
Audit Questions	
Whether the Access Control Policy exists, management has approved it, owners are responsible for reviewing and maintaining it and it is published to all personnel.	
Whether the policy expresses management's commitment to information security and clearly defines the controls that must be in place.	
Whether a review process exists to ensure that the policy is updated to reflect changes such as significant security incidents, changes to the business process and changes to the IT&T system.	
Importance of the Control	
This policy is an essential part of the defence against unauthorised intrusions into the IT&T systems. Since the organisation possess some information that is classified as HIGHLY PROTECTED, it is essential that it have adequate security, especially from the Internet.	
Requirements for Compliance	
The policy must be available to all personnel. It must be regularly reviewed and updated as necessary.	

Audit Steps	**Findings**	**Compliance**
7. Has the policy been approved by management?	Management have approved the policy.	Yes
8. Does the policy have a designated owner?	The Information Security Manager owns this policy.	Yes
9. Has the policy been reviewed on a regular basis?	The policy has not been reviewed since its implementation.	No
10. Changes are made to the policy as necessary.	No changes have been identified for this policy as yet.	Yes

This checklist is used to ensure that the controls to protect critical information assets are protected against unauthorised intrusions. The policy will be updated in response to significant security incidents and to other significant changes that could open vulnerabilities to the system.

4.11 Password Management Policy Checklist

ISO 17799 Reference: 9.2.3	**Control:** User password management

Audit Questions		
Whether a Password Policy exists, management has approved it, owners are responsible for reviewing and maintaining it and it is published to all personnel.		
Whether the policy expresses management's commitment to information security and clearly defines the controls that must be in place.		
Whether a review process exists to ensure that the policy is updated to reflect changes such as significant security incidents, changes to the business process and changes to the IT&T system.		
Whether personnel are using strong passwords.		
Importance of the Control		
Passwords are the first line of defence in an IT&T system. If users select weak passwords, or reveal their passwords to others, the system can easily be compromised.		
Requirements for Compliance		
The policy must be available to all personnel. It must be regularly reviewed and updated as necessary. Passwords must not be easily revealed.		
Audit Steps	**Findings**	**Compliance**
1. Has the policy been approved by management?	Management have approved the policy.	Yes
2. Does the policy have a designated owner?	The Information Security Manager owns this policy.	Yes
3. Has the policy been reviewed on a regular basis?	The policy has not been reviewed since its implementation.	No
4. Changes are made to the policy as necessary.	No changes have been identified for this policy as yet.	Yes
5. Verify operation of operating system password controls by attempting to choose passwords that do not comply with the policy.	Non-compliant passwords cannot be selected.	Yes
6. Audit passwords on a regular basis using L0phtcrack.	Passwords are audited monthly. The rate of cracking passwords has reduced from 80% to 20%.	Yes

4.12 Patch Management Checklist

ISO 17799 Reference: 10.4.1	**Control:** Control of operational software
Audit Questions	
Does a policy exist outlining the need to apply patches to critical IT&T systems in a timely manner?	
Importance of the Control	

Vulnerabilities are being announced on a regular basis for many computer systems and exploits are becoming available faster and faster. Consequently, it is essential to patch critical systems as quickly as possible.		
Requirements for Compliance		
Where possible, critical IT&T systems must be patched before exploits are available.		
Audit Steps	**Findings**	**Compliance**
1. Does a policy exist for patch management?	The policy is included in Section 8.3.2 of the Enterprise Information Security Policy and a procedure is included in the SOPs Manual.	Yes
2. Does a subscription exist to a vulnerability alerting service?	The Information Security Manager subscribes to the SANS @Risk service and to the Microsoft Security Bulletin service.	Yes
3. Are patches installed in a timely manner?	Patches are installed promptly after testing.	Yes

Part 5 Act

5.1 Update the ISMS to Include the Check and Act Processes

The ISMS for this organisation was developed based on AS/NZS 7799.2:2000. This original version of the Australian standard did not include the Plan Do Check Act cycle. Consequently, the ISMS needs to be updated to include ongoing checking and updating processes.

5.2 Incident Management

The Security Committee maintains an Incident Register and reviews it during the regular meetings. As significant incidents occur, information security policies and procedures will need to be reviewed to see if changes and improvements need to be made to prevent similar incidents from occurring again in the future. This is in accordance with Sections 6.3 and 8.1.3 of ISO 17799.

5.3 Review the Threat and Risk Assessment

The TRA needs to be reviewed at leats annually, or when any of the following occur:

- Significant changes to business operations;
- Significant changes to IT&T systems;
- Significant vulnerabilities are publicised;
- A significant security incident occurs.

5.4 BCP Testing and Updating

A continuous process of testing and updating the BCP must be established to ensure that it is effective and that it is kept current with changes to the business and IT&T systems. This testing should include a combination of paper-based tests and realistic scenarios being enacted out and must involve all relevant staff.

As problems with the existing BCP are identified during testing, the BCP must then be reviewed to determine the best way of addressing the problems. The BCP will then need to be updated, with the updates being approved by the Deputy CEO and distributed to all relevant staff.

Each member of staff who has responsibilities in relation to the implementation of the BCP must be provided with a hard copy and must store this at home so it is readily available in the case of an emergency. An additional copy must be stored off-site with the backup tapes.

Testing and updating the BCP are requirements of Section 11.1.5 in ISO 17799.

5.5 Improve Security Awareness Training Program

The scope of the Security Awareness Training Program needs to be expanded to include all information security policies in use by the organisation. As new policies are developed, the Training program must continue to grow.

A mechanism must be established to track who has attended training sessions and to follow up on those who have not attended. Additionally, the training program must be incorporated into the induction training program for new employees.

5.6 Review Policies

Information Security Policies need to be reviewed at least annually, or when any of the following occur:

- Significant changes to business operations;
- Significant changes to IT&T systems;
- Significant vulnerabilities are publicised;
- A significant security incident occurs.

5.7 UPS Configuration

Older file servers must be configured to shutdown gracefully in the event of an extended power failure.

5.8 Improve Backup System

The computer backup system must be improved to ensure that all servers are reliably backed up according to the defined schedule. This may require involving the assistance of the relevant vendors to resolve technical issues.

A schedule must be established for testing the ability to restore data from backup tapes.

Appendix A References

1. SANS G7799 Course Material;
2. AS/NZS 7799.2:2003 – "Information Security Management";
3. ISO/IEC 17799:2001 – "Information Technology – Code of Practice for Information Security Management";
4. AS/NZS 4360.2000 – "An Approach to Risk Management";
5. Defence Signals Directorate's "Australian Government Information Technology Security Manual (ACSII 33)", http://www.dsd.gov.au/library/infosec/acsi33.html;
6. NSW Office of Information and Communications Technology's "Guide to Labelling Sensitive Information", http://www.oit.nsw.gov.au/pdf/4.4.33.Guide.pdf;
7. SANS Policy Project "Password Protection Policy", http://www.sans.org/resources/policies/Password_Policy.pdf

Appendix B Proposed Policies

B1 Enterprise Information Security Policy

Due to the size of the Enterprise Information Security Policy, the entire document could not be included here. Below are some relevant extracts from it.

2.3.1 Security requirements in outsourcing contracts

Covered by Policies: Code of Conduct, Disclosure of Information Policy, Use of Communication Devices Policy, and Service Level Agreement

To maintain the security of information when the responsibility for information processing is outsourced to another organisation, outsourcing arrangements shall address the risk, security controls and procedures for information systems, networks and/or desk to environments in the contract between parties.

5.1.4 Security of computer rooms

Covered by policies: Code of Conduct, Access Policy, System Operation and Procedures Manual

Computer rooms supporting critical business activities shall have good physical security with the design of the room taking into account the possibility of damage from various sources.

The following measures shall be implemented:

- Key facilities shall be sited away from areas of public access;
- The lobby directory and internal telephone list shall not identify the location of the computer facilities;
- Hazardous and combustible materials shall be stored securely at a safe distance from the computer room. Computer supplies such as stationery shall not be stored within the computer room until required;
- Fallback equipment and back-up media shall be sited at a safe distance to avoid damage from a disaster at the main site;
- Appropriate safety equipment shall be installed, such as heat and smoke detectors, water sensors, fire alarms, fire extinguishing equipment and fire escapes. Safety equipment shall be checked regularly in accordance with manufacturers' instructions. Employees shall be properly trained in the use of safety equipment;
- Emergency procedures shall be fully documented and regularly tested.

5.2.3 Power supplies

Covered by policies: Informal

Equipment shall be protected from power failures or other electrical anomalies. An uninterrupted power supply (UPS) shall be installed for equipment supporting critical business operations. UPS equipment shall be regularly tested in accordance with the manufacturer's recommendations.

5.2.4 Cabling security

Covered by policies: Informal

Power and telecommunication cabling carrying data or supporting IT services shall be protected from interception or damage.

The following security measures shall be applied to reduce these risks within the organisation's premises:

- Measures shall be taken to protect network cabling from unauthorised interception or damage, for example by using conduit or by avoiding routes through public areas;
- For exceptionally sensitive or critical systems, consideration should be given to additional measures such as:
  - Use of data encryption;
  - Installation of armoured conduit and locked rooms or boxes at inspection and termination points;
  - Use of alternative routings or transmission media.

6.4.2 Data back-up

Covered by policies: System Operation and Procedures Manual, Computer Systems Backup and Monitoring Policy

Back-up copies of essential business data and software shall be made in accordance with the Computer Systems Backup and Monitoring Policy. Adequate back-up facilities shall be provided to ensure that all essential business data and software can be recovered following a computer disaster or media failure. Back-up arrangements for individual systems shall meet the requirements of business continuity plans:

- A minimum level of back-up information, together with accurate and complete records of the back-up copies, shall be stored at a remote location, at a sufficient distance to escape any damage from a disaster at the main site. At least three generations of back-up data shall be retained for important business applications;
- Back-up data shall be given an appropriate level of physical and environmental protection, consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site;
- Back-up data shall be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary;
- Data owners shall specify the retention period for essential business data and also any requirement for archive copies to be permanently.

6.5.2 Network security controls

Covered by policies: System Operation and Procedures Manual, Position Descriptions, Service Level Agreements

A range of security controls is required in our computer network. The Network Security Administrator shall ensure that appropriate controls are established to ensure the security of data in our network, and the protection of connected services from unauthorised access.

In particular:

- Operational responsibilities for networks shall be separated from computer operations, where appropriate;
- Responsibilities and procedures for the management of remote equipment, including equipment in user areas, shall be established;
- Special controls shall be established, if necessary, to safeguard the confidentiality and integrity of data passing over public networks, and to protect the connected systems;
- Computer and network management activities shall be closely coordinated; both to optimise the service to the business and to ensure that security measures shall be consistently applied across the IT infrastructure.

7.1.2 Documented access control policy

Covered by policies: Access Control Policy, System Operation and Procedures Manual

Requirements for access control are outlined in the access control policy. This policy shall authorise the lowest level access privileges for a new user, based on advice from team managers. It shall give IT staff a clear statement of the business requirements for system access, in order to implement and maintain an effective level of control of access to IT services and data. However, each business application owner (see Appendix A) will need to develop a clear access policy statement that defines the access rights of each user or group of users, in particular where higher level privileges are to be authorised.

The policy shall take account of the following:

- The security requirements of individual business applications.
- Policies for information dissemination and entitlement, eg the `need to know' principle.

Access to core network applications, such as the Exchange Server, files servers etc, shall be authorised by the security committee.

7.2.4 User password management

Covered by policies: Use of Communication Devices, User Password Policy, System Operation and Procedures Manual

Passwords are the principal means of validating a user's authority to access a computer service. A formal management process shall control the allocation of passwords. In particular it shall:

- Require users to sign an undertaking to keep personal passwords confidential;
- Ensures, where users are required to maintain their own passwords and that they shall be provided initially with a secure temporary password that they shall be forced to change immediately. Temporary passwords shall also be provided when users forget a password, always subject to positive identification of the user;
- Conveys temporary passwords to users in a secure manner. Conveyance of passwords through third parties or through unprotected (clear text) electronic mail messages shall not occur. Users shall acknowledge receipt of passwords.

8.3.2 Control of operational software

Covered by policies: System Operation and Procedures Manual

Strict control shall be exercised over the implementation of software on operational systems.

The following controls will be implemented to minimise the risk of corruption of operational systems:

- The updating of the operational program libraries shall only be performed by the nominated librarian upon authorisation from the IT support manager for the application;
- If possible, only executable code should be held on operational systems;
- Executable code shall not be implemented on an operational system until evidence of successful testing and user acceptance is obtained, and the corresponding program source libraries have been updated;
- An audit log shall be maintained of all updates to operational program libraries;
- Previous versions of software shall be retained as a contingency measure;
- Vendor supplied software used in operational systems shall be maintained at a level supported by the supplier;
- Software patches shall be applied when they can help to remove or reduce security weaknesses.

8.4.2 Change control procedures

Covered by policies: System Operation and Procedures Manual

In order to minimise the corruption of information systems, there shall be strict control over the implementation of changes. Formal change control procedures shall be implemented. They ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of the system that are necessary for their work, and that formal interdisciplinary agreement and approval for any change shall be obtained.

9.1.1 Objective

Covered by policies: Business Continuity Plan

The Business Continuity Plan is designed to protect critical business processes from the effects of major failures or disasters.

The Business Continuity Plan shall outline the process for the speedy restoration of critical business processes and services in the event of serious business interruptions. Such interruptions may be caused by natural disasters, accidents, equipment failures, deliberate action, and loss of supplied services or loss of utilities. As part of the Business Continuity Planning process, an analysis of risks to the Office shall be conducted. Risk minimisation strategies shall be identified and where appropriate shall be implemented. All business areas shall participate in the analysis. Risk minimisation strategies shall limit the consequences should a threat be realised, and ensure speedy resumption of essential operations.

B2 Access Control Policy

OVERVIEW

The Organisation relies on a variety of information to perform its duties, some of which is sensitive. It is essential that the confidentiality of this sensitive information be maintained.

PURPOSE

The purpose of this policy is to ensure that only authorised users have access to sensitive information possessed by the Organisation.

Use of System Utilities

Only authorised users shall have access to installation packages for system utilities.

The number of authorised users for system utilities shall be kept to a minimum. Authorisation shall only be granted where the use is justified against a business need.

The use of all system utilities shall be logged.

The proper use of all system utilities shall be documented.

System utilities that are no longer necessary shall be removed.

System utilities include, but are not limited to applications such as the following:

- Password auditors;
- Network performance testers;
- Security auditing tools;
- Network scanners.

Access Control to Program Source Code

Application source code shall be stored separate from the operational system.

The Database Administrator shall be responsible for application source code.

Access to source code shall be provided only when approved changes are to be made.

Updating of source code shall be performed only by the Database Administrator.

Data Encryption

Notebooks shall be protected with a proven standard encryption algorithm. The type of encryption used shall be reviewed annually and upgraded as technology allows.

SCOPE

The scope of this policy includes all personnel who are responsible for backing up and monitoring any computer system that resides at any Organisation facility, has access to the Organisation network, or stores any Organisation information.

POLICY

User Access Management

Login Requirements and Procedures

User identification names shall consist of the user's first initial followed by their surname. In the event of a conflict with another user identification, the middle initial shall be used after the first initial where possible; alternatively the first two letters of the users first name shall be used.

System and default usernames loaded and required by the operating system shall be changed if possible and assigned a different password from that which was loaded.

Usernames required for services without login requirements shall be configured not to allow logins.

Usernames for services not in use shall be deleted from the system if possible. Alternatively, they shall be disabled.

Guests and Other Users

Guests and other non-Organisation users shall be given access to the network and its resources by the Team Manager and the Network Security Administrator.

The sponsor shall provide the user with access to the Organisation's security policies and procedures with an understanding that they are responsible for following them. The Team Manager and Network Security Administrator shall be responsible for monitoring the guest user.

Guest usernames shall be assigned only for the duration that access is required. Usernames shall be revoked following the end of the access requirement.

Login Banners

All login screens, displays, and other banners appearing during the login or authentication process shall not contain any information identifying anything about the operating environment.

Banners displayed during the login and authentication process shall include the state that usage of the system constitutes agreement with the company's security policies and procedures. They will also include a non-disclosure agreement stating that the users actions can be monitored and recorded.

Session Restrictions

Users shall lock and secure workstations when not in use during working hours and log off at the end of the working day. Administrators shall create procedures to ensure that unused workstations are secured by logoff or other means when they are idle for a reasonable period of time.

Review of User Access Rights

Team managers shall be provided with a list of users who have access to the business systems and data they own at least every six months to review users' access capabilities.

Team managers shall be provided with a list of administrators for the business systems and data they own at least every three months for review.

Application Access

Information Access Restriction

Users shall not have rights to change access controls to any Organisation information or applications.

Assigned business owners are responsible for approving access by users to the Organisation's information and applications under their care. User access to Organisation information applications shall be granted only after approval from the relevant business owner.

Administrative staff shall perform their regular duties with a standard (non-administrative) user account and shall be provided with a unique and separate administrative account to be used only when required. All usage of administrative accounts shall be audited and monitored.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Issue	Date	Description
0.1	July 2002	First draft for IT review

B3 Computer Systems Backup and Monitoring Policy

OVERVIEW

The organisation relies on a number of computer systems to perform its duties. Failure to backup and monitor these systems correctly may result in the loss of the Organisation's entire corporate data. It is the responsibility of Organisation employees operating the backup systems and monitoring the computer systems to do so according to the procedures outlined below.

PURPOSE

The purpose of this policy is to ensure the correct and secure backup and monitoring of Organisation computer systems.

SCOPE

The scope of this policy includes all personnel who are responsible for backing up and monitoring any computer system that resides at any Organisation facility, has access to the Organisation network, or stores any Organisation information.

POLICY

System Backups

Backup tapes shall be handled in the following manner:

- Backup tapes shall be duplicated, with one copy stored locally and one copy stored off-site at the Organisation approved storage facility.
- At least one copy of each backup tape shall be retained for the following durations:

Backup Type	Storage Duration
Monthly (Grandfather)	2 years
Weekly (Father)	1 month
Daily (Son)	1 month

- When backup tapes have exceeded their lifetime, or are seen to be producing errors, they shall be erased in a secure manner before being disposed of.

Backups shall be scheduled using a GFS rotation scheme in the following manner:

- Full backups shall be scheduled to run at least weekly, and outside normal business hours.
- Differential backups shall be scheduled to run daily on all remaining business days, and outside normal business hours.

When major system changes are to be performed, at least one additional full backup of any systems that may be affected shall be performed immediately prior to undertaking the planned changes.

In the event of an incomplete backup, the cause of the problem shall be immediately diagnosed and rectified, if possible. In the event that any critical files (e.g. system files, Organisation data files, etc) may have not been successfully backed up, the incomplete backup shall be scheduled to run again immediately.

In the event of unexpected operational or technical difficulties, the Network Administrator shall be contacted first, followed by the IT Manager.

On a daily basis, results of all backups shall be checked and recorded in the log sheets for each respective file server. These logs are to be kept in the designated shelf in the secure server room.

System restart and recovery procedures for use in the event of system failure

System Monitoring

All security-related and system events on critical or sensitive systems shall be logged and audit trails saved and kept online for a minimum of 1 week.

An audit shall be performed on these logs at least weekly.

Security-related events shall be reported to the Network Security Administrator, who will review logs and report incidents to IT management. Corrective measures shall be prescribed as needed. Security-related events include, but are not limited to:

- Port-scan attacks;
- Access failures;
- Review of logon patterns for indications of abnormal use or revived user Ids;
- Allocation and use of accounts with a privileged access capability;
- Tracking of selected transactions;
- The use of sensitive resources;
- Anomalous occurrences that are not related to specific applications on the host.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Issue	Date	Description
0.1	July 2002	First draft for IT review

B4 Network Security Policy

OVERVIEW

This policy defines the standards required to connect the Organisation's information technology network to any external network, either private (such as third party government agencies) or public (such as the Internet). These standards are designed to minimise the potential exposure to the Organisation's network from damages that may result from unauthorised use of Organisation resources. Damages include the loss of sensitive or confidential data, intellectual property, damage to public image, or damage to critical Organisation internal systems.

PURPOSE

The purpose of this policy is to ensure that only authorised and controlled access to the Organisation network is permitted.

RESPONSIBILITY

The Security Manager is responsible for ensuring that appropriate and approved controls are placed between the Organisation network and any external networks.

POLICY STATEMENT

External Gateway

The external gateway of the Organisation network shall be configured to meet the Department of Commerce "Guide to Labelling Sensitive Information" guidelines. Since the network stores information labelled "Highly Protected", the gateway shall be comprised of two different firewalls, running on different operating systems from DSD's Evaluated Products List. The firewalls shall:

- Deny all traffic unless it is explicitly allowed;
- Only permit traffic that has been approved by the Security Committee and serves a specific and necessary purpose;
- Be patched in a timely manner;
- Be reviewed and audited on a regular basis to ensure correct configuration;
- Have logs stored in a manner allowing them to be permissible as evidence in a court of law;
- Be configured so that only the Network Security Administrator or a person suitably qualified and authorised by the Network Security Administrator can make changes.

Changes shall only be made to the firewalls with the authorisation of the Security Committee and of the PCCM WAN forum where appropriate.

Monitoring

A correctly configured IDS shall be running at all times to provide immediate notification of attempted intrusions into the network. The IDS shall:

- Be patched and updated in a timely manner;
- Be reviewed and audited on a regular basis to ensure correct configuration;

- Have logs stored in a manner allowing them to be permissible as evidence in a court of law.
- Be configured so that only the Network Security Administrator or a person suitably qualified and authorised by the Network Security Administrator can make changes.

Changes shall only be made to the IDS with the authorisation of the Security Committee.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Issue	Date	Description
0.1	July 2002	First draft for IT review

B5 Password Policy [7]

Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the Organisation's entire corporate network. As such, all Organisation employees (including contractors and vendors with access to Organisation systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Organisation facility, has access to the Organisation network, or stores any non-public Organisation information.

Policy

General

- All system-level passwords must be changed on at least a monthly basis;
- All production system-level passwords must be part of the InfoSec administered global password management database;
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 30 days. The recommended change interval is every four months;
- User accounts that have system-level privileges granted through group memberships or applications must have a unique password from all other accounts held by that user;
- Passwords must not be inserted into email messages or other forms of electronic communication;
- Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private", "system", and the organisation's name and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2);
- All user-level and system-level passwords must conform to the guidelines described below.

Guidelines

1. General Password Construction Guidelines

Passwords are used for various purposes at Organisation. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few

systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters;
- The password is a word found in a dictionary (English or foreign);
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc;
  - Computer terms and names, commands, sites, companies, hardware, software;
  - The organisation's name, "sydney" or any derivation;
  - Birthdays and other personal information such as addresses and phone numbers;
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc;
  - Any of the above spelled backwards;
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret).

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z);
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./);
- Are at least eight alphanumeric characters long;
- Are not a word in any language, slang, dialect, jargon, etc.;
- Are not based on personal information, names of family, etc.;

Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

2. Password Protection Standards

Do not use the same password for organisation accounts as for other non-organisation access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various organisational access needs.

Do not share organisation passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential Organisation information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE;

- Don't reveal a password in an email message;
- Don't reveal a password to the boss;
- Don't talk about a password in front of others;
- Don't hint at the format of a password (e.g., "my family name");
- Don't reveal a password on questionnaires or security forms;
- Don't share a password with family members;
- Don't reveal a password to co-workers while on vacation.

If someone demands a password, refer him or her to this document or have him or her call someone in the Network Security Administrator.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least monthly (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to the Network Security Administrator and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by the Network Security Administrator or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

3. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups;
- Should not store passwords in clear text or in any easily reversible form;
- Should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

4. Use of Passwords and Passphrases for Remote Access Users

Access to the organisation’s Networks via remote access is to be controlled using a one-time password authentication.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Revision History

Issue	Date	Description
0.1	9 July 2002	First draft for IT review