Information Technology Policy and Procedures

1 INTRODUCTION

This document sets out the way in which the business uses, develops and maintains Information Technology (IT) to assist in the achievement of the Objectives and Goals of the business.

This policy also covers the various steps and processes we expect to have in place to ensure we have an effective Cyber Security system to prevent unauthorised access, use and exploitation of data we hold on our clients and on our business practices and processes.

The effective, efficient use and protection of information and systems within a Financial Services business is a major issue for our business.

The appropriate management of this task is also a requirement of the Corporations Act as spelt out by ASIC in RG104 (RG104 - Licensing - Meeting The General Requirements) and therefore an ongoing necessity for us to operate within the Financial Services industry.

Australian Privacy Principle 11 requires us to take reasonable steps to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure. In addition the National Data Breach scheme requires us to notify both the individual involved and the Office of the Australian Information Commissioner (OAIC) where an Eligible Breach occurs. For further information on this please refer to our Privacy Policy and Procedures

Information Technology is specifically addressed within both our Risk Management Policy and Procedures (Risk Management Policy and Procedures) and our annual Business Plan for this very reason.

All staff and Authorised Representatives must be familiar with and comply with this Policy and Procedure, understand the importance the business places on the effective operation of our Policies and Procedures and are encouraged to look for improvements to our procedures.

2 UPDATES

These Policy and Procedures are updated on a regular basis. Any material changes to these Policy and Procedures will be advised by management either via Email or at our regular Staff meetings.

This document and associated forms etc. are accessible in soft copy via our computer network. We do not store these documents in hard copy. All information can be immediately accessed on the computer network and will be guaranteed to be up to date at all times.

When you see an opportunity to improve a procedure kindly make the suggestion known to your manager/supervisor as we all have a responsibility to improve our standards, individually and as a Company.

3 SOFTWARE SUPPLIERS / DEVELOPMENT AND SELECTION

The purchase or engagement of any third party software that has the potential to impact on the delivery of our services to our clients must be subject to our Outsourcing Policy and Procedures (Outsourcing Policy and Procedures).

In the selection and use of any information technology the security and adequacy of the software and data must be paramount in the minds of both management and staff.

The business does not perform any software development functions and all software is purchased from reputable suppliers within their chosen software areas.

It is against this policy to develop software programs internally or to purchase or engage software and software suppliers that do not have a proven track record within our industry and that attest to the security of their products from external attack.

Where relevant the purchase contracts for software and systems must address the issue of system maintenance/development and specific response expectations in the event of system failure.

4 PROTECTING OUR INFORMATION TECHNOLOGY

Where possible and practical key computer hardware is to be located in secure areas with access limited to relevant staff. Where cost effective such equipment is to be protected from power surge by hardware. Access to the secure location is to be limited to as few staff as practical.

The ITC will allocate responsibility for locking up the secure area (where applicable) where servers and backup tapes are stored. A backup person should be organised to cover times when the primary person is unavailable because of holidays, illness etc.

Where equipment is out in the open, or is left unattended for periods of time, desktop machines should be locked to the desk or to a portion of the building structure where possible and practical.

Special care needs to be taken with the security processes for all portable electronic equipment or remote equipment with the ability to access our network or to store company / client data.

Specifically all such equipment must have a commercial grade password to be able to access the machine. In the event of any such equipment being lost or stolen, staff and representatives are to immediately advise the ITC who will take the necessary steps to deactivate the specified equipment's access to our network.

This will include changing any network Wi-Fi passwords (where the stolen/lost equipment holds such information) as well all user passwords for any staff that may have used the stolen/lost equipment.

In addition all hardware that has the ability to access our network remotely must be able to be locked out of the network regardless of the password access provided to the network. In other words there must be hardware security in place as well as the software security.

The business operates Anti-Virus software across our network and as part of the induction process new staff and representatives are trained in the identification of potential virus files and what is required to be done when a virus is detected.

Firewalls have been installed within the computer network to protect the IT system from attack from external sources.

Under no circumstances are staff or representatives to introduce software programs or external data to the IT system without prior approval of the ITC.

To ensure the security of our data all client data and any other data that the business will rely on going forward must be stored on selected resources to enable the effective back up and subsequent recovery of such data in the event of a disaster.

Any disaster that impacts our Information Technology systems has the potential to have a catastrophic result for the operation of the business.

The business therefore has developed and implemented Disaster Recovery Policy and Procedures (Disaster Recovery Policy and Procedures)

To ensure the business continues to have the IT capability to meet the needs of the business, an inventory of all IT hardware and software is maintained by the business as part of our Asset Register.

Where we have a Wi-Fi network it is to be secure, encrypted, and hidden. To hide our Wi-Fi network the wireless access point or router is to be set up so that it does not broadcast the network name, known as the Service Set Identifier (SSID). There will also be a commercial grade password applied to the Wi-Fi router.

5 INFORMATION TECHNOLOGY RESOURCES

We have nominated an Information Technology Co-Ordinator (ITC1) as well as a backup person (ITC2) where relevant with the responsibility for the management and maintenance of all IT systems within the business. These staff are identified in our Organisation Chart.

The ITC's will be provided with the necessary training to be able to effectively perform their role.

We have will also engaged a reliable IT provider (details available from the ITC) to provide professional service, support and expertise to the business to ensure our IT systems operate to an industry standard and to assist the ITC in technical areas that are beyond experience and expertise of our ITC.

5.1 ROUTINE ACTIVITIES

The responsibility for the day to day management of our IT infrastructure is shared between our ITC and our external IT provider. Ultimate responsibility for the effective implementation of this policy rests with our ITC.

There should be clear and documented agreement between the ITC and the IT provider of the agreed responsibilities and task of both parties.

The specific skills, roles and responsibilities of the ITC and the IT provider include:

- Controlling all staff and representative access to the Information Technology environment including passwords.
- Ensure staff and representatives are only provided access to IT areas / data required to perform their role and that a workable hierarchy of authority is in place so that staff and representatives are only authorised to perform tasks which they are required / trained and expected to perform.
- Ensuring staff and representatives store all relevant data on the nominated data storage devices.
- Computer backups are completed as per schedule and before any major software or hardware changes are implemented.
- Virus software is correctly installed and kept up to date on a weekly basis for all key equipment.
- Any firewall that has been installed operates on all computers/network to ensure that the computer system is protected.
- Selecting/Installing/Replacing/Maintaining IT hardware.
- Supporting external contractors with software and hardware modifications and upgrades to ensure all security patches are promptly installed.
- Ensure access to data and communication servers and control tables is limited to the ITC and delegated staff.

- Ensuring default passwords on software supplied from vendors is updated immediately upon receipt.
- Ensure all staff and representatives utilising password protected software update their passwords on a regular basis.
- Ensure that no software/hardware is able to be set to have “auto password complete” activated in any situations.
- Maintaining relevant IT records (refer below).
- Ensure access for departing staff and representatives is removed accordingly.
- Develop and maintain standard specifications for all hardware and software utilised within the business.
- Develop a thorough understanding of our Disaster Policy and Procedures (Disaster Recovery Policy and Procedures) and implement work practices that are conducive to an effective recovery from a disaster.
- Consider the cost /benefit and implement where appropriate routine Penetration Tests on all external facing software (e.g. websites) where such websites have the potential to provide access to client or corporate data. Penetration Testing is an authorised attempt for certified ethical ‘hackers’ to breach your system in order to identify its vulnerabilities and to safely close any flaws that real cyber criminals may exploit.
- Maintain full details of computer network configuration, specification and software for use in the event of a disaster.
- Review the currency and appropriateness of our hardware and software, response times, downtime and any complaints received from staff regarding our Information Technology resources.
- Nominate and train a replacement person responsible for Back Up procedures when the ITC will not be available.
- Check that all company equipment which is physically on the same network as our Servers has had all capability of loading CD’s/DVD’s/USB Drives removed or deactivated.
- Maintain a record of all hardware and software that has the ability to access our network remotely and regularly review the usage of such hardware to assess whether such ongoing access is warranted and relevant.

5.2 Disaster Response Activities

To see that full IT functionality is restored in the minimum time, with particular focus on an effective restoration of data from our back up facilities.

Liaise with critical suppliers to determine the causes of failure and to develop plans to restore functionality.

Liaise with the Disaster Recovery Co-Ordinator and the Responsible Manager(s) to update them on status and to plan the return to normal business, as systems become available.

6 IT PROVIDER SERVICE LEVEL AGREEMENTS

Our IT provider will be required to enter into a Service Level Agreement (SLA) with us. The IT provider will usually supply their own standard agreement which can be customised / adjusted to reflect our requirements.

As a rule of thumb, if our IT provider does not have a standard agreement then we should seriously consider whether they have the necessary systems, processes and controls to consistently deliver the IT services we require to the level we expect.

The following is a checklist of items that we would expect to see in any SLA:

- Expected response times for incidents (X% in less than 10 minutes)
- Supply of current contact information for all relevant staff, including after hours contact.
- Target uptimes (that are monitored) for Servers / PC's and key network infrastructure.
- Availability to support required system software changes as required.
- Supply, installation and monitoring of antivirus / firewall / security patches / upgrades within X days of release / availability.
- Implementation and support for industry standard software and hardware security access including two factor identification where possible/practical, automatic time based log off process and lock out on maximum number of unsuccessful login attempts.
- All external data communications (email's / remote access / data feeds etc) are subject to industry standard data encryption protection.
- Supply, installation of new replacement hardware / software.
- Supply, installation, monitoring and testing of back up processes.
- Support for remote worker access, including provision of secure remote access software and deployment of hardware as required.
- Documentation of IT environment at a level that would enable a replacement IT provider to quickly and efficiently take over the role.
- Website hosting / management and support.
- List of routine activities that are responsibility of the IT provider not listed above.
- An attestation that the security procedures in place at the IT provider are in line with Industry Codes.
- An obligation that the supplier informs us of any possible data breach;
- The supplier immediately remedies the data breach and complies with our directions when dealing with a data breach; and that we have control over notices to OAIC and affected individuals.
- Who has the right to determine whether a data breach is likely to result in serious harm;
- Where a data breach has occurred, which party must complete an Office of Australian Information Commissioner (OAIC) assessment within the 30 days period; and which party will pay for the assessment.

7 STAFF AND TECHNOLOGY

The majority of staff and representatives have access to a PC or related equipment. The company has networked our computer facilities and linked the system to both e-mail and Internet access.

Access to these facilities is for predominantly business purposes only and not for private matters. Our view is that all data, information, messages etc. that are transacted over our network and hardware is not subject to any privacy restrictions that might usually apply to individuals.

Any usage of Our IT equipment to access, create, store or otherwise facilitate the use of pornographic, sexually explicit material or other data that would be considered inappropriate by community standards is a Serious Breach of our Policy and Procedures and will result in immediate termination for the staff or representative involved.

For any staff or representatives that may be located in NSW we will ensure we comply with the NSW Workplace Surveillance Act 2005.NSW Workplace Surveillance Act Guidelines

The ITC will randomly monitor traffic to and from the server as well as the overall network.

The ITC will also advise all staff and representatives of any common viruses that are known to be in the wild and impacting clients or other industry sites.

All staff and representatives are to be advised at induction and on a regular basis thereafter that they are not to open emails that could reasonably be expected to contain spam or phishing software and under no circumstances are they to accept any prompts to "upgrade/install/refresh/run" any software except where specifically instructed to by the ITC or the IT provider.

Where access to the office computer systems etc. is required as part of staff member's or representative's job, they will be given appropriate password access and are expected to treat this password as confidential. Staff and representatives are not to share passwords etc.

In many cases staff and representatives will be provided with network storage facilities to be used to store files created by the user. It is important they use these network facilities as they are protected by our back up procedures. Files stored on a local PC may be lost and irrecoverable in the event of a major IT disruption.

Staff and representatives are able to utilise the Internet for work related purposes only. Specific permission must be granted to a staff member or a representative for personal use of the Internet. Accessing of offensive sites and downloading of non-work related data and software is against company policy.

We also require that staff and representatives use only CD/DVD/USB Drives supplied by the company. Exterior storage devices risk the introduction of viruses that may affect the network or company files and information.

Even though we have taken all reasonable care to ensure safety and a virus free computer environment, we are all aware of the problems a virus can cause.

Deviation from these rules will be considered serious misconduct and could ultimately result in the termination of the services of the staff member or representative involved.

Further information on the usage of Emails and Viruses are included in the Staff Policy and Procedures (Staff Policy and Procedures)

8 BASIC QUESTIONS AND PROBLEMS

Our investment in desktops, laptops, tablets etc. and software licenses is significant. It is no use investing in these unless our people can make use of the hardware and the software.

While support and advice from colleagues is a good way to learn, we don't want the entire office to stop work while everyone crowds round one person's desk as they try to create a table of contents in Word.

The ITC has allocated responsibility to one person (with a backup if necessary) to replenish stocks of paper, toner etc. for printers and fax machines.

Any computer hardware or software questions or problems are to be referred to the ITC initially. The ITC will determine the steps to be taken if they are unable to address the issue raised.

9 MAINTAINING RECORDS

Our software licenses are valuable. It's easy to install software on a machine and "forget" that it is there. It is also easy to forget what service contracts we have in place for your equipment. Finally, it is easy to forget to renew a domain name. Domain names are cheap, but very valuable. If we don't renew our domain name, someone else can register it, and we will struggle to get it back.

The ITC in conjunction with our external IT provider is responsible to keep a list of what software is installed on every machine, with what licences to ensure that the business is complying with the Licence agreements and is protecting the business's assets.

The ITC in conjunction with our external IT provider is responsible to keep a list of what domain names and web hosting arrangements we have, with expiry dates and ensure there is a system in place to remind us to renew domain names (We should renew them about 3 months in advance of the deadline).

The ITC is responsible for maintaining a list of all service contracts. Only one person is permitted to call a vendor for service.

10 CREATING, MAINTAINING AND DELETING USERS

New staff and representatives need to be added as new users to the network, and just as importantly, old staff and representatives need to be removed as soon as they leave the business.

The ITC in conjunction with our external IT provider is responsible to add new users and remove users to/from the network.

The system for adding new users should enable a new user to be added to the network so they can be productive from the day they start work (without having to use someone else's password to access the network).

The ITC in conjunction with our external IT provider maintains a central registry of passwords to business-critical files or applications, or to retrieve passwords from departing employees. For example, an accounts clerk may have passwords to the on-line banking, or a staff member may have password-protected individual documents that the business will need.

The person who oversees the departure of a staff member is responsible for informing the ITC that the employee is leaving. The ITC in conjunction with our external IT provider is responsible for disabling that user from the network as soon as they receive notice.

11 CREATING AND RE-SETTING PASSWORDS

All new users on the network will need a password that they can change for their own needs. And whether we like it or not, users forget passwords and can be locked out of the network.

The network should have a "five strikes and you're out" policy: if a user gets the password wrong five times in a row, the user is locked out of the network.

The ITC in conjunction with our external IT provider should be able to re-set the password of someone who is locked out within a very short time (say, 10 minutes). The ITC should nominate a backup for this task to cover meal breaks, leave and other absences.

The network operating system and all sub systems should be set up so as to require users to ideally change their network password monthly, but in any situation no less frequently than quarterly.

Password rules should be appropriate to the circumstances but not be so difficult that users are tempted to write them down. Our default position is that all passwords should be minimum 10 character length, with passwords to contain at least three of the following: number, upper case character, lower case character and special character.

12 INSTALLING NEW EQUIPMENT

In a small business, it is tempting to buy new equipment without having thought about how it will be installed. You don't want the entire business to come to a stop as 5 people try to install a new scanner "just like the one we have at home"!

We must ensure that the equipment we buy is suitable for a business network environment. Not all equipment suitable for home use will run on a business network.

When we buy new equipment, consideration must be given to arranging for the vendor to install it. While it will cost a little, it may be cheaper than having our staff fumbling at a task that is not their area of expertise.

To reduce complexity, we will endeavour to limit our purchases to a few brands and types of equipment that we trust and are familiar with.

We must ensure that new drivers (e.g. printer drivers) are installed when we buy new equipment. Even if the new printer "seems to work" with the old drivers, make sure that everyone is using the same drivers for the same printer.

All new equipment installed should be checked to ensure that any facilities to connect unauthorised equipment to the unit have been deactivated e.g. CD/DVD Drives and USB drives.

13 SHARED FOLDERS, PERMISSIONS AND DISK QUOTAS

Shared folders allow groups of staff and representatives to access the same files. Disk quotas restrict the amount of data that one employee can store on a server. There are security and performance implications for both.

We need to ensure the business has appropriate rules in place so that people can see the data they need for their job, but data is generally secured.

The ITC in conjunction with our external IT provider has been allocated the job of managing shared folders and granting permission to individuals or groups to see the files in those shared folders.

Permissions to access shared folders are reviewed regularly and permissions are deleted when they are no longer needed (perhaps because someone changed roles within the business).

Where appropriate, disk quotas are in place that limit the space that an individuals' files can take up on servers. The business server is not the place for individuals to store large files they have downloaded from the web!

All business data should be stored on the server where it can be secured, and backed up.

14 SECURITY PATCHES

As long as malicious users try to breach systems through security holes in software, software vendors will be issuing security patches.

We have considered and decided on a policy to install all security patches as soon as they are made available.

The ITC (in conjunction with our external IT Provider) is responsible for downloading, assessing (if necessary), and deploying security patches for the operating system and applications (line-of-business applications, back-office systems and desktop applications).

Our external IT Provider is required to regularly check that security patches are being deployed appropriately.

15 INTERNET CONNECTIONS – ISP

For our business, the connection to the internet is vital. The market remains volatile and ISPs are routinely dropping prices, increasing service speeds and broadening service offerings.

We may not want to change ISP every 6 months, but we should stay aware of changes in this market.

In choosing an ISP, we explore a wide range of possible vendors to get the services you need and the best value for money.

The ITC in conjunction with our external IT provider is responsible for managing the technical aspects of connecting to the internet and deals with the ISP about problems with the connection.

The ITC in conjunction with our external IT provider is also responsible for regularly checking competitive pricing and service offerings.

16 INFORMATION REPORTING

All software systems utilised by the business must be capable of providing the relevant business and management reports required to effectively manage the business.

Relevant exception reports must be included in all reporting functions to ensure early warnings are provided to management when processes or functions are not meeting expected levels.

17 SECURITY

We must ensure the security of data, especially confidential and sensitive material collected within our Information Technology systems.

To this end all staff and representatives are to be issued with appropriate system access that enables them to perform their required tasks and only access to data that is appropriate to their role.

The use of system passwords, user id's and a hierarchy of access will be implemented wherever possible to support this approach.

18 DATA BACK UP AND RETRIEVAL

The following data backup and retrieval processes are to be implemented and reviewed for effectiveness on a regular basis by the ITC in conjunction with our external IT provider.

- At the end of each day a backup process to a stable data storage facility is to be performed, involving all business data held on our server(s).

- Where this involves a portable media (Tape/Disk/Portable Drive) back up, the portable media is to be removed from the site as soon as is practicable, but no later than the following business day.
- Each day's back up data must be retained as an absolute minimum until the successful completion of the next day's back up process. In an ideal situation there will be backups available for the last 5 days at any one time as well as backups for a nominated day of the week for the past 4 weeks.
- Where significant software or hardware installations are planned a full back up process and restore test is to be implemented prior to the installation. These backups are to be kept for a minimum of 5 days after the completion of such installations.
- The backup data created at month end must be retained at a minimum until the successful completion of the next months back up process. In an ideal situation we should have 11 months of back up accessible at any one time.
- The backup data created at the financial year end is to be retained for seven years.
- All back up storage processes must include clear identification of the date of the back up to facilitate effective and speedy restore processes.
- A comprehensive test of the backup and restore facilities is to be conducted on a quarterly basis or as detailed in the Business Plan.
- A review of data storage on the network should be conducted on a quarterly basis to ensure all business data is being stored on the Server(s) and not on individual PC's.
- Any ongoing or consistent problems encountered with either Back Up or Restore processes must be actioned and resolved as a matter of absolute urgency.

19 SPAM WORDING

Where we plan to send marketing material to clients we may have a standard SPAM Wording that should be used for all clients where we plan to send outbound email marketing material. The ITC will be able to advise on the location of this document. It is based on the following template - Spam Wording Template.

20 WEBSITE PRIVACY

Where we operate a Website we must ensure that all client information collected via the website is secure. We must therefore ensure that our Website developer has the necessary skills and expertise to meet this obligation.

21 WEBSITE CONTENT

The following information should be included in a prominent place in all business websites:

- Our AFS Licence Number should be displayed on the Home Page.
- A link(s) to the following information should be included on our Home Page
  - Our Financial Services Guide.
  - Information about our membership of the Australian Financial Complaints Authority (AFCA) and its role and contact details where relevant.
  - Our Internal Complaints resolution processes where applicable.
  - Information on relevant Industry Codes that we follow or subscribe to.

All internet generated product quotes should clearly and separately disclose any fees applicable that are included in the total amount quoted to the client. In addition our FSG, any relevant Product Disclosure Statement (PDS) or Policy Wording and our standard Important Notices including Duty of Disclosure notice should also be made accessible at the time the quotation is provided and prior to the client being able to make a decision to purchase the relevant product.

Social media sites should include a link to our full Website with a wording similar to the following: For further information including statutory notices, please see our website www.########.com.au

22 CYBER SECURITY INCIDENT RESPONSE PLAN

22.1 OVERVIEW

This incident response plan defines what constitutes a security incident and outlines the incident response phases. This incident response plan documents how information is passed to the appropriate personnel, assessment of the incident, minimising damage and response strategy, documentation, and preservation of evidence. The incident response plan defines areas of responsibility and establishes procedures for handling various security incidents.

22.2 PURPOSE

This policy is designed to protect the organisational resources against intrusion and minimise any disruption or damage that an intrusion causes.

22.3 INCIDENT RESPONSE GOALS

- Verify that an incident occurred.
- Maintain or Restore Business Continuity.
- Reduce the incident impact.
- Determine how the attack happened.
- Prevent future attacks or incidents.
- Improve security and incident response.
- Prosecute illegal activity.
- Keep management informed of the situation and response.

22.4 INCIDENT DEFINITION

An incident is any one or more of the following:

- Loss of information confidentiality (data theft)
- Compromise of information integrity (damage to data or unauthorized modification).
- Theft of physical IT asset including computers, storage devices, printers, etc.
- Damage to physical IT assets including computers, storage devices, printers, etc.
- Denial of service.
- Misuse of services, information, or assets.
- Infection of systems by unauthorized or hostile software such as a virus.
- An attempt at unauthorised access.
- Unauthorised changes to organisational hardware, software, or configuration.

- Reports of unusual system behaviour.
- Responses to intrusion detection alarms.

22.5 Incident Responsibility

The Information Technology Co-Ordinator (ITC) is the primary person for ensuring an appropriate response is made once an incident has been identified. In the absence of the ITC, the responsibility falls to the Responsible Manager(s) (RM) of the business.

22.6 Incident Discovery

This occurs when someone discovers something not right or suspicious. This may be from any of several sources:

- Helpdesk
- Intrusion detection system
- A system administrator
- A firewall administrator
- A business partner
- A monitoring team
- A manager
- The security department or a security person.
- An outside source.

22.7 Incident Notification

The ITC is to be immediately informed of any incident. Our default position is that any incident reported should be assumed to be a real threat to our business operations and managed accordingly until such time it is proven to be benign.

The ITC should immediately contact our IT Supplier for support in addressing any incident. The Responsible Managers (RM) and the management of all areas potentially impacted by the incident are also to be immediately advised of the situation.

22.8 Incident Severity

The ITC is to categorise the incident into the highest applicable level of one of the following categories:

- Category one - A threat to public safety or life.
- Category two - A threat to sensitive data
- Category three - A threat to computer systems
- Category four - A disruption of services

The severity of the incident should be used as part of the decision making and priority setting within the response framework.

22.9 Analysis and Assessment

Many factors will determine the proper response including:

- Is the incident real or perceived?
- Is the incident still in progress?

- What data or property is threatened and how critical is it? For example does data include: Personal information, sensitive information, driver's license number, Credit Card Number (including PIN's CSV's, Expiry dates), bank account number (including PIN or other access information), Medical information or health insurance information
- Is the exposed data encrypted?
- What is the impact on the business should the attack succeed? Minimal, serious, or critical?
- What system or systems are targeted, where are they located physically and on the network?
- Is the incident inside the trusted network?
- What type of incident is this? Example: virus, worm, intrusion, abuse, damage.

22.10 Response Strategy

In deciding the response required once an incident is reported the following factors need to be considered:

- Is the response urgent?
- Can the incident be quickly contained?
- Will the response alert the attacker and do we care?

22.11 Containment

Take action to prevent further intrusion or damage and remove the cause of the problem. This may involve:

- Disconnecting the affected system(s).
- Changing passwords.
- Blocking some ports or connections from some IP addresses.
- Taking down websites / intranets / servers etc.

22.12 Prevention of Re-Infection

To prevent subsequent reinfection we need to know how the intrusion happened.

We need to determine the source of the intrusion whether it was email, inadequate training, attack through a port, attack through an unneeded service, attack due to unpatched system or application.

Take steps to prevent an immediate re-infection which may include one or more of:

- Close a port on a firewall
- Patch the affected system
- Shut down the infected system until it can be re-installed

Other steps that may be required include:

- Re-install the infected system and restore data from backup. Be sure the backup was made before the infection.
- Change email settings to prevent a file attachment type from being allowed through the email system.
- Plan for some user training.
- Disable unused services on the affected system.

22.13 Restore Affected Systems

Restore affected systems to their original state. Be sure to preserve evidence against the intruder by backing up logs or possibly the entire system. Depending on the situation, restoring the system could include one or more of the following

- Re-install the affected system(s) from scratch and restore data from backups if necessary.
- Make users change passwords if passwords may have been sniffed.
- Be sure the system has been hardened by turning off or uninstalling unused services.
- Be sure the system is fully patched.
- Be sure real time virus protection and intrusion detection is running.
- Be sure the system is logging the correct items

22.14 Documentation and Preservation

Document what was discovered about the incident including how it occurred, where the attack came from, the response, whether the response was effective.

Make copies of logs, email, and other documentable communication. Keep lists of witnesses.

Notifying proper external agencies:

- The police if prosecution of the intruder is possible.
- The Office of the Australian Information Commissioner if a privacy breach is involved.
- ASIC if the incident is likely to lead to a significant breach.

22.15 Damage Assessment and Review

Assess the damage to the organisation and estimate both the damage cost and the cost of the containment efforts.

Review response and update policies. Plan and take preventative steps so the intrusion can't happen again.

Consider:

- Whether an additional policy could have prevented the intrusion.
- Whether a procedure or policy was not followed which allowed the intrusion, then consider what could be changed to be sure the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident response procedures detailed and cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection of the current infection? Are all systems patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?