CCI
Catholic Church
Insurance

risksupport

FACT SHEET

Developing an IT Security Policy

An organisation that poorly or inadequately manages its online security faces many risks including unauthorised access to their data and transmission of viruses.

The consequences can be devastating. Damage to reputation, interruptions to valuable services, data and financial losses, decreased productivity, liability for financial compensation and regulatory penalties are all possible outcomes.

Establishing processes and procedures to treat or manage online risk can greatly reduce the likelihood of an incident occurring. Workers should be involved in the development of these documents and appropriate information and training needs to be provided so that everyone understands what is required.

An IT Security Policy is a must-have for any Catholic organisation. It specifies how the organisation will protect the integrity of its network and comply with industry standards and audit requirements.

The objectives of an IT Security Policy are to:

- Secure physical assets including computers, laptops, servers and portable storage devices such as USBs and hard drives from unauthorised access, theft, breach of policy, confidentiality and accidental damage
- Protect the security, confidentiality and integrity of any data or information stored on the network
- Protect the organisation from liability
- Protect the reputation of the organisation and its people.

What should the policy cover?

An IT Security Policy needs to be tailored to an organisation's individual circumstances. Ask yourself: who has access to your computers and equipment? How is the security and integrity of passwords ensured? What are your students and workers responsibilities in relation to private information stored on your system? Is your system protected from malicious software or individuals who might seek to gain access? Can you ensure the safety of data? How can you be sure the security systems you have in place are up-to-date?

While the specific details of an IT Security Policy are unique to each organisation, there are basic elements common to almost everyone. A policy would typically include:

A policy statement

- Provides a clear outline of what the policy is for, the potential risks and the role users have to play in reducing them.

Details regarding enforcement

- Provides information regarding who will be responsible for enforcing the policy and likely outcomes of a breach, which may include official warnings, counselling and termination of employment.

Information on roles and responsibilities

- Sets out who is responsible for enforcing, monitoring and auditing the policy and to whom the policy applies.
- Outlines procedures to follow if any part of the policy is unclear.

Network security procedures

- **The use of antivirus software**

  Computer viruses and malware (malicious or malevolent software) are software programs designed to interfere with computer operation by recording, corrupting and deleting data. They often have the ability to copy themselves and spread to other computers and the internet. Antivirus software is designed to defend a computer against viruses and malware.

- **The use of patching**

  A patch is a piece of software designed to correct a specific problem within a computer program, application or operating system. The Federal Government's Defence Signals Directorate (DSD) 2013 rated patching the second most effective security practice an organisation could perform. Most major software companies periodically release patches, which are generally downloaded from the internet. It is possible to configure systems to automatically update as soon as patches are made available.

- **The use of firewalls**

  A firewall is a hardware or software-based security system which monitors information going in and out of a computer or network including emails, files and data. As the name suggests, a firewall is a virtual barrier capable of preventing the spread of dangerous or malicious material from outside the network, into the network. Information is analysed to determine whether it should be allowed though.

- **Backup strategy**

  Backup describes the process of copying and archiving data to ensure its security. A backup strategy sets out which data will be backed up, how often and to where. It also outlines the procedure for recording the movement of backup files and for retrieval. Backup strategies and retrieval methods must be regularly tested and should integrate with overall business continuity plans.

- **Reaction and recovery plans**

  Having a plan in place for how an organisation will respond to and recover from an incident is essential. Whether they're reacting to a virus, server failure or security breach, organisations need procedures in place to get them back to regular operations as quickly as possible, maintain access to critical business systems and protect their data.

- **Restriction of administrators**

  Administrator is the highest level of permission granted to a user within a network and as such, an administrator has enormous influence. They can install software, change configuration settings and alter the operating environment. Malicious software (malware) often seeks to gain administrative privileges to compromise computers. Minimising the number of people with administrative privileges makes it more difficult for malware to spread and provides a more stable, predictable environment.

- **The use of passwords**

  A password is a string of characters used to prove identity or to gain access to any number of company systems including the network, email system and the internet. Poor or weak passwords are easily cracked and put the entire system at risk. All organisations need to set a clear standard for creating, protecting and changing passwords and ensure passwords are strong, secure and protected.

Physical security procedures

- **Security of premises**

  Securing physical access to equipment in the workplace is important. Premises must be safe and secure to prevent unauthorised access. Only authorised personnel should be permitted to gain access to computers, servers, systems and applications.

- **Security of portable equipment**

  The security of portable devices such as laptops, tablets and mobile phones, along with storage devices like USBs, hard drives and CDs must also be considered.

Review schedule

An IT Security Policy should be reviewed regularly or at least annually. It should also be reviewed after an incident has occurred, after major changes to systems and equipment are made or training exercises have occurred.

Communication and training

Employees, students, volunteers and contractors need appropriate training on the specifics of the policy. This could form part of the general induction program, be delivered to a group during professional development training, via an online training program or as a one-on-one briefing, depending on people's age, experience and location.

Practical help

Regardless of size, location, activities and operations, an organisation that uses computers and/or the internet should also consider implementing the following basic policies and developing appropriate procedures to support them.

- Password Policy
- Email Usage Policy
- Internet Usage Policy
- Firewall Policy
- Content Management Policy
- IT Reaction and Recovery Policy

CCI has a number of useful publications on this and many other topics available at **www.risksupport.org.au** or by calling the risk*support* Helpdesk on **1300 660 827**.

They include:

- Managing Online Risk
- Developing a Password Policy
- Developing a Firewall Policy
- Developing an Email Usage Policy
- Developing an Internet Usage Policy
- Developing a Content Management Policy
- Developing an IT Reaction and Recovery Plan
- Managing Risk in Catholic Organisations Conducting a Risk Assessment, Developing a Risk Treatment Plan
- Business Continuity Management.

Assistance is also available via State and Federal Government agencies and other sources including:

Your IT service provider

Defence Signals Directorate
www.dsd.gov.au/infosec/top35mitigationstrategies.htm

www.staysmartonline.gov.au

www.cybersmart.gov.au

National Computer Emergency Response Team
www.cert.gov.au

Legislation, guidelines and codes of practice

ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements

ISO/IEC 20000-1:2011 Information technology - Service management - Part 1: Service management system requirements

AS/NZS ISO/IEC 27002:2006, ISO/IEC 27002:2005 (Information technology - Security techniques - Code of practice for information security management)

AS/NZS ISO/IEC 27001:2006, ISO/IEC 27001:2005 (Information technology - Security Techniques - Information Security Management Systems – Requirements).

AS/NZS ISO 31000:2009 Risk Management Principles and Guidelines

HB 266:2010 Guide to Managing Risk in Not-For-Profit Organisations

Cyber Insurance

CCI's Cyber Insurance can protect you from the fallout of a range of cyber-crime and computer-based activities. Cyber events including computer malware, data breaches, cyber extortion threats and denial of service attacks can all lead to losses and claims being made against you.

If you would like more information speak to your Account Executive, visit **www.ccinsurance.org.au** or call **1800 011 028**.

For assistance with risk management, please contact the risk*support* Helpdesk on:

1300 660 827
helpdesk@risksupport.org.au
www.risksupport.org.au

www.risksupport.org.au
Catholic Church Insurance Limited
ABN 76 000 005 210, AFSL no. 235415
GPO Box 180 Melbourne 3001

Important Notice: This publication is intended to provide a summary and general information only to clients of Catholic Church Insurance Limited. It does not constitute, and should not be relied on as advice or considered as a comprehensive coverage of the topics discussed. You should seek professional advice tailored to your own circumstances.

risksupport