CCI Catholic Church Insurance

risksupport

FACT SHEET

Developing a Firewall Policy

A firewall is a hardware or software-based security system which monitors information going in and out of a single computer or computer network (via the internet) including emails, files and data. Information is either blocked or allowed to pass through the firewall, depending on the settings, preventing the spread of dangerous or malicious material. They are a critical element of an organisation's overall IT security framework.

Many computers and other hardware such as modems and routers have in-built firewalls. Software firewalls need to be installed on a computer or network and can be configured according to specific needs. In larger organisations a firewall is often installed on a designated computer separate from the rest of the network. This is known as a gateway or proxy server.

A Firewall Policy sets clear standards for establishing and maintaining firewalls and ensures everyone who uses a network is aware of the risks, knows what's required of them and understands how this will all be monitored and enforced.

The objectives of a Firewall Policy are to:

- Provide clear guidelines and accountabilities for installing, configuring and monitoring a firewall
- Protect the confidentiality and integrity of information stored on the network
- Protect the organisation from liability
- Protect the reputation of the organisation and its people.

What should the policy cover?

A Firewall Policy needs to be tailored to an organisation's individual circumstances. While the specific details of a Firewall 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 including 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.
- Sets out who is responsible for installing, monitoring and updating firewalls.
- Provides details of procedures to follow for example:
  - If there is a suspected breach of a hardware or software firewall
  - To request a change to firewall settings or rules
  - If any part of the policy is difficult to understand or unclear.

Information on firewall configuration

- Provides details of what information may flow into a computer or network.
- Provides details of what information may flow out of a computer or network.

Review schedule

A Firewall 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, volunteers and contractors who are involved in the delivery, management or service of an organisation's IT system need appropriate training. 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.

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 Client Relationship Executive on **1800 011 028**

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

1300 660 827

helpdesk@risksupport.org.au

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

risksupport