KAON SecurITy

# IT Policy System

Kaon SecurITy specialise in the human factors side of information security and provide services to Local Government, Central Government and commercial enterprises in New Zealand and Australia.

Kaon SecurITy is acknowledged for its regional leadership in IT policy deployments and technical security auditing services.

Established in 2004, Kaon SecurITy is the professional services division of MPA New Zealand Ltd.

**www.kaonsecurity.co.nz**

Today organisations rely heavily on their electronic environment for the day-to-day processing and management of business. Issues of information management, confidentiality, competitive edge and profitability are intrinsically linked. And in terms of security, unfortunately information in the electronic world has not yet received the same level of respect as the paper document achieved in its time.

The first step towards creating a secure electronic environment is to define the rules and guidelines for managing, operating and using corporate information systems. This step is critical and involves developing policies and procedures that document the management and control of the electronic information.

To be successful, Information Systems Security Policies must be based on common sense and all staff, contractors and third parties need to be required to understand their obligations associated with the use of a company's information.

As ANZ Consulting Partners for Protocol Policy Systems, Kaon SecurITy work with their generic set of policies and procedures which are then uniquely tailored to match your organisation's environment, to ensure the policy matches what you do.

The policies are provided in a user-friendly, web format that is easily deployed in any intranet environment. Text, graphics and formatting within the Protocol Policy System are customised during the build process to suit the culture of the business.

## WHAT THE POLICIES DO

- Help protect the assets of a business
- Provide an organisations' computer security framework
- Provide a uniform level of control and guidelines for management
- Communicate security messages in a format that is easily available and understood
- Advise staff about their responsibilities to the policies
- Endorse commitment of the CEO and senior management in protecting valuable information assets.

## HOW THE POLICIES ARE ORGANISED

The policies are set out by category for Users, Managers and Technical members of staff. This allows staff easy access to the policies that relate to them without needing to read other technical jargon.

Everyone who uses the computer systems, communications systems or networks that make up the electronic environment must be familiar with the policies listed under the User menu. Managers should be familiar with policies listed under both the User and Management menus while Technical staff need to be familiar with the policies listed under the Technical menu.

## OBLIGATIONS TO STAFF

Organisations are responsible for educating and training staff on how to use the computer systems correctly and for imposing the importance of security for handling corporate information which may be confidential or sensitive.

Managers often have little time or don't have the resources or skills to develop a comprehensive policy that documents onsite practices and helps achieve best practice. Kaon SecurITy helps companies achieve their IT policy objectives by developing a set guide to using specific electronic information systems, which all staff can have easy access to.

## STAFF RESPONSIBILITIES

It's the responsibility of every staff member, temporary employee, contractor and third party user to ensure they read, understand and comply with policies when using organisational computer systems, electronic information, and networks. Having policies set in place eliminates misuse of systems.

## COMPLIANCE WITH ISO 27002

ISO 27002 is the code of practice for Information Security in Australia, New Zealand and many other countries around the world and sets the criteria for achieving best practice security management. Adopting ISO 27002 provides evidence that security is taken seriously by management and stakeholders can have confidence that the Council is acting responsibly to protect itself from the risk of a serious security breach.

## THE POLICIES

The Protocol Policy System includes 25 comprehensive policies covering all aspects of information system usage. All policies have drop down explanations, links to relevant standards and, where applicable, cross reference to statements in other associated policies.

## KEEPING UP TO DATE

Policy documentation, as part of an overall IT Security Framework is not static. It changes as the IT environment evolves and changes wither because new personnel bring new approaches, the technology is updated or the organisation itself adapts culturally. In some organisations there is no one onsite that can be allocated the task of maintaining the content of the IT policies or introducing new ones – IT Departments don't have the resources and Human Resources don't have the knowledge. It is possible that IT policy documentation is neglected until it bears no resemblance to what actually occurs onsite and this situation may actually create security vulnerabilities. Having no policies at all is sometimes better than having policies that are inaccurate or outdated.
Our Support and Maintenance Plan provides:

- Fixes for anything that is not functioning correctly in within the Policy System
- The ability to upgrade to the latest version of the Protocol Policy System when updates are released includes new policies or capabilities, at no cost.
- Phone support for assistance with any queries or issues regarding the functioning of the software.

KAON SecurITy

Your IT security services partner

www.kaonsecurity.co.nz

MPA New Zealand Ltd, Level 1, 4 Waipuna Road, Po Box 62049, Mt Wellington, Auckland 1644, New Zealand

t. NZ +64 9 570 2233 | t. VIC +61 3 9913 3248 | t. QLD +61 7 3194 3664 | t. NSW +61 2 9098 8206 | f. +64 9 570 2355 | e. sales@kaonsecurity.co.nz