PROTOCOL
POLICY SYSTEMS

IT POLICY MANAGEMENT AS A SERVICE

Creating A Secure Computing Environment

Delivered “as a service” on an annual subscription basis

- Our experts help you create and maintain your organisation-wide IT Security policies.
- Rapidly deliver a comprehensive suite of 25+ policies, customised and branded to your organisation.
- Automatically cross reference your policies to relevant industry standards such as ISO27002, ISO22313, ISO27017, ISO29151, PCI-DSS and PSN.
- Demonstrate good corporate governance and regulatory compliance – GDPR.

The first step towards creating a secure computing 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.

THE CHALLENGE

Many organisations do not have someone in-house that has the subject matter expertise or experience in writing IT Policy. Often policies are revisited and reviewed every 5-8 years using a "big bang" approach. Someone is nominated to tackle this laborious and time consuming exercise and commences a re-write or edit of the content. Should the "big bang" exercise start and finish completely the policies are not typically then maintained so that ongoing changes in business requirements, technology and standards are reflected.

POLICY MANAGEMENT AS A SERVICE

Protocol Policy Systems has developed a generic set of policies and procedures for Local Government which are then uniquely tailored to match your organisation's environment, to ensure the policy matches what you do.

Our Policy Management as a Service cloud-based subscription solution allows a Local Authority to deliver up to date IT Security Policies to all staff including technical and management roles, eliminating the overhead of creating and maintain those policies in house.

All the hard work of gaining expert knowledge, developing and maintaining policies to keep them current and mapped to standards such as ISO, PCI, PSN is taken care of by the PPS team on behalf of our customers. We become your IT Security Policy Partners.

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 such as for User, Manager or 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 the 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. Protocol's IT Policy System 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 STANDARDS

Different industries and jurisdictions look to adopt standards to help them optimise their business operations or to comply with regulatory requirements. ISO 27002 is the code of practice for Information Security in many countries including the UK, Australia, and New Zealand. It 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.

THE POLICIES

The IT 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

We provide ongoing updates to the Information System Policies under our subscription plan. This may include the addition of new policies, refreshes or changes to old policies based on newly discovered vulnerabilities or weaknesses and amendments to compliance standards.

If you introduce new technology and need policies to support them we can write these for you to incorporate into your current IT Policy System ensuring your policy system matches the current operating environment. Any changes or additions to your system are mapped to the appropriate standards while we action updates.

PROTOCOL POLICY SYSTEMS

Tel: 01604 762 992
Email: sales@protocolpolicy.com
WEB: www.protocolpolicy.com
MAIL: 8a Basset Court, Grange Park
Northampton, NN45EZ

Socitm
Delivering digital leadership

A joint venture between Protocol Policy Systems & SOCITM