

# POLICY MANAGEMENT AS A SERVICE

## Creation, delivery and management of IT Policies made easy

- Our experts help you to create and maintain your organisation-wide IT Security policies
- Rapidly deliver a comprehensive suite of 25 policies, customised and branded to your organisation
- The policies are automatically cross referenced to relevant industry standards and best practice including ISO, PCI, PSN and Cyber Essentials
- Demonstrate good corporate governance, regulatory and legislative compliance, and protect customer data – GDPR

**T**he first step towards creating a secure computing environment is to develop policies and procedures that document the management and control of digital information.

To be successful, Information Systems Security Policies must be written using easy to understand language so that all parties understand the requirements and their obligations associated with the use of company information.

## FIVE COMMON CHALLENGES

- No one in-house has the subject matter expertise or experience in writing IT Policies
- Existing policies are seldom reviewed to keep them up to date with changes in business and technology usage requirements
- Writing and maintaining policy content in-house or on a bespoke basis is laborious and expensive
- Stakeholder and user engagement requires a lot of management and effort
- Monitoring and measuring user engagement with the content is difficult

## POLICY MANAGEMENT AS A SERVICE

Protocol Policy Systems have developed a generic set of policies, which are then uniquely tailored to align with your organisation's practices.

Policy Management as a Service (PMaaS) is a cloud-based subscription solution available in 3 versions – Lite, Essentials and Premium. PMaaS allows an organisation to deliver up to date IT Security Policies in under 5 weeks, eliminating the overhead of creating and maintaining 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-DSS and CE+ is taken care of by our experts on behalf of our customers.

Once in place, PMaaS makes the process of engaging and monitoring stakeholder and user interaction with the content both easy and visible.

## WHAT DOES PMAAS DO

- Helps protect the assets of a business
- Provides an organisation's IT security framework
- Provides a uniform level of control and guidelines for management
- Communicates security messages and training in a format that is easily available and understood
- Advises team members about their responsibilities to the policies
- Endorses the commitment of the CEO and senior management to protect valuable information assets and improve security posture

## HOW ARE THE POLICIES ORGANISED

PMaaS includes 25 comprehensive policies covering key aspects of information system usage. All policies are written in plain English, with drop down explanations, links to relevant standards and, where applicable, cross referenced to statements in other associated policies. The policies are set out by category for User, Manager, or Technical team members, which allows easy access to the policies that specifically relate to them.

## COMPLIANCE WITH STANDARDS

Organisations adopt standards to help them optimise their business operations, manage risk, or comply with regulatory requirements. As an example, ISO 27002 is the code of practice for Information Security in many countries including Australia, New Zealand and the U.K. It sets the criteria for achieving best practice security management. Mapping of policies to standard and best practice guidance provides evidence that security is being taken seriously by management, and stakeholders can have confidence that the organisation is acting responsibly.

## USER ENGAGEMENT


PMaaS has been designed to address many of the shortcomings of in-house bespoke policy initiatives which may not address stakeholder and user engagement considerations.

Examples of options the service provides include:

- Stakeholder input around policy wording can be captured in the system throughout the service delivery phase
- Presenting enrolled users with specific content from the overall policy framework to review
- Invite third parties that are required to work with your systems and data to create a login and view the policy content
- Onscreen review and acceptance of policies – time efficient with no paperwork required
- The Primary Administrator can generate user interaction reports
- Insite Compliance reporting provides further detailed visibility
- Supporting materials to help users to develop and improve their understanding of the need for good security behaviours – security awareness videos, topic index, glossary of terms, top tips

## KEEPING UP TO DATE

Under the PMaaS subscription plan all policy content is automatically kept up to date by us, as are the standards, mappings, and supporting material. Our subject matter experts are also available to adapt policies for customers as their business requirements change.

 UK +44 845 241 0099  
NZ +64 9 570 2233

 sales@protocolpolicy.com

 www.protocolpolicy.com



A joint venture with  Socitm