PROTOCOL
POLICY SYSTEMS

THE IMPORTANCE OF IT POLICIES

Table of Contents

Introduction

IT Security Policies play a critical and strategic role in ensuring corporate information is kept safe. This whitepaper answers a number of questions covering the importance of developing and deploying IT Security Policies properly, the business benefits gained, process considerations in terms of stakeholder input, typical policy development shortcomings and ongoing policy management considerations.

Why are IT Policies important?

1. Information security is all about keeping corporate information safe. Policies address the requirement to protect information from disclosure, unauthorised access, loss, corruption and interference and are relevant to information in both electronic and physical formats.

   Information security can be defined by three things:

   - Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes
   - Integrity - data must not be altered or destroyed in an unauthorised manner, data accuracy and consistency must be preserved regardless of changes
   - Availability - information must be accessible and useable on demand by authorised entities

2. Organisations are reliant on information and communications technology to run and build their business. This may be in support of the activities of the business (financial systems, logistics, CRM etc) or an online business channel where customers make purchases or payments for goods and services.

3. It is important that these systems are used, operated and managed efficiently and effectively. This ensures business continuity and will enable the organisation to meet legal, regulatory and statutory requirements.

4. The organisation must define and communicate its expectations for the appropriate use of these systems, so that they remain available for business purposes and their use does not bring the organisation into disrepute.

5. Technology never stands still. With the proliferation of new technology it is more important than ever for organisations to understand what they want their IT environment to look like and how their information should be used.

6. Many of the problems around information leakage can be avoided through appropriate use of information systems.

7. Documented policies and procedures take the guess work out of information security and enable an organisation to manage business risks through defined controls that provide a benchmark for audit and corrective action.
8. Without documented policies and procedures, each and every employee and contractor will act in accordance with their own perception of acceptable use, system management will be ad-hoc and inconsistent. Staff will be unaware as to whether they are acting within the organisation's risk appetite or not.
9. Security attacks against organisations are increasing both in number and sophistication, we must ensure our systems can be protected against these threats. The first step in achieving this is to document the rules and guidelines around system management, operation and use. By complying with these documented rules and guidelines, organisations are taking steps to protect their systems and their people from a security threat.
10. Effective information security policies protect staff as much as the organisation.

Risk Considerations

Organisations provide access to their valuable assets such as vehicles, machinery and building facilities. In doing so, it is expected management and staff fully understand the terms of use, health and safety considerations and in some cases the need to complete operator training.

However, the same level of expectation is often not well detailed for management and staff, regarding how they interact with valuable technology and information assets. Typically, the investment afforded to developing and maintaining IT security policies and procedures is minimal, which creates a business risk.

The business catalyst, for implementing information security policies and procedures should not be an IT related issue or disaster, but a considered and well thought out approach, based on business impact analysis, risk assessment and risk mitigation strategies, driven from the top of the organisation down.

The risks of not defining acceptable use and management standards, for information and information systems include:

- Damage to reputation.
- Financial repercussions due to remediation requirements.
- Loss of business.
- Misuse of data - yours or customers.
- Loss of data – yours or customers.
- System unavailability.
- Legal or regulatory issues.

What are the business benefits?

As noted above, defining and implementing IT security policies helps an organisation to identify and manage business risks.

Having well defined policies and procedures that are communicated to staff, that are reviewed and updated regularly to keep up with changes in the environment, return the following benefits to the business:

- Provide a security and acceptable use framework for the organisation.
- Help to protect the information systems and information assets of the organisation.
- Provide a uniform level of control and guidelines for management.
- Deliver one consistent information security message to all.
- Communicate IT security and acceptable use policies and guidelines to users.
- Provide-a benchmark for monitoring and measurement compliance.
- Assist with staff issues relating to the misuse of the technology or the information.
- Meet internal obligations of auditors and risk managers.

Who should be involved in the development of IT Policies?

The CIO, IT Manager, Network Administrators and System Administrators should all be involved in the development of the Policies and Procedures. Input from Human Resources and Information Managers is also recommended. We also recommend input from Risk and Legal staff if these roles exist within the organisation. Ultimately, Senior Executives and the Management Team should sign off the policies.

How do organisations typically manage their policies today?

Many organisations have a basic Email and Internet Use Policy. They do not comprehensively define their information and information systems management and use expectations. If they have policies, they are usually a couple of word documents published somewhere on the organisation’s intranet. If policies have been developed, they may be out of date, available in hardcopy only and not published in such a way that they are readily available to the wider user community. Email and Internet Use Policies may be included by Human Resources during staff induction as a handout but, there is no reiteration of the policies on an ongoing basis. Often there is no training on information security and typically no ongoing security awareness program.

What are the common shortcomings we see in the area of policy development?

1 The DIY approach:
Writing effective policies takes months or even years and therefore it is often put in the too hard basket.

2 Copying a best practice manual, often doesn't correlate with how the business operates in practice:
The policies are not meaningful and are soon disregarded.

3 Not going through the review process:
The first draft provided is often a generic policy system, taking the time to review and further customise the policy statements ensures that they are appropriate for the organisation.

4 Not keeping the policies up to date with changes to operational practices and technology.

5 Not communicating the final policies to staff or publishing the policies so that they are readily available to the wider user community.

How does the Protocol Policy System address these shortcomings?

1 Security policies (sometimes renamed standards or protocols) contained within the Protocol Policy System address the business need to protect confidential and sensitive information from disclosure, unauthorised access, loss, corruption and interference and is relevant to information in both electronic and physical formats.

2 Protocol's *Policy Management as a Service* solution, takes the pain away from defining and deploying IT security policies. It will enable organisations to meet their internal risk and audit requirements. The CIO or IT Manager is able to focus on other priorities. Feedback from organisations that have been through our delivery process which includes a 3-day review say it is the best 3 days they have ever spent as it provides them with an introspective view of their current environment.

3 The Protocol Policy System provides comprehensive IT Security policies and supporting documents in a total solution that only requires a minimal time commitment to manage from the organisation. Our cloud-based offering is cross referenced to several best practice standards for compliance purposes. No training is required to get it set up and to use it and our subscription model encompasses all ongoing maintenance work to keep the system up to date. The content is customisable so customers decide the wording and content that is appropriate to their organisation.

What types of organisations use the Protocol Policy System today?

The IT Security policies in the Protocol Policy System are applicable to any organisation that uses Information and Communications Technology in carrying out its business. It is totally scalable, platform agnostic and no training is required to get it set up and to use it. The system caters for customers with less than 20 staff to those with thousands of users. A wide range of customer~~s~~ types use the system including Central Government agencies, Local Government agencies and organisations in sectors including Banking, Finance, Insurance, Utilities, Infrastructure, Transport, Retail and Education.