THE IMPORTANCE OF IT POLICIES

Table of Contents

Introduction

An innovation and transformation strategy's success can be determined by the use of the right team to deliver a practical digital program that enables organisations to overhaul their legacy IT systems, improve capability, and strengthen their cyber security posture.

A framework of IT security policies is key in helping clients to better leverage data and emerging technologies in order to design and deliver secure customer-centric services. IT security policies provide the foundation for developing a good cyber security posture, and will ultimately help to ensure the success of a digital program.

This whitepaper provides a guide to fundamental IT security policy topics, such as the importance of properly developing delivering and maintaining IT security policies; risk considerations; business benefits; stakeholder input; typical shortcomings; and ongoing management considerations.

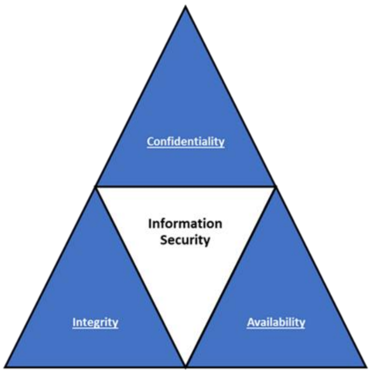
The importance of properly developing, delivering and maintaining IT security policies

IT security policies help an organisation implement strategies to address IT security threats and vulnerabilities whilst also detailing how to recover from a network intrusion. Further key considerations are -

1. Information security is primarily concerned with keeping data safe. Policies address the requirement to protect information from disclosure, unauthorised access, loss, corruption and interference.

   Information security can be defined by three principals:

- Confidentiality - information must not be made available or disclosed to unauthorised individuals, entities, or processes
- Integrity - information must not be altered or destroyed in an unauthorised manner 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 technology to run and build their businesses, including support of business activities such as engagement channels where customers can make enquiries, applications, purchases, or payments for goods and services. Policies efficiently and effectively communicate how these systems are to be operated and managed, ensuring business continuity. They also enable the organisation to meet legal, regulatory, and statutory requirements.
3. Technology never stands still. In this ever-changing world of technology it's important for organisations to understand and adapt to a dynamic digital environment, and the resulting changes in their risk profile. IT security policies assist an organisation to be more agile and effective in their adoption of technology, whilst managing associated risks.
4. The volume of data that organisations collect and store continues to increase. Data usage, sharing, and leakage risks can be addressed through the use of documented IT security policies which take the guess work out of information security.
5. Without access to a suite of comprehensive IT security policies, employees and contractors act in accordance with their own perception of acceptable use. Data and system management may be ad-hoc and inconsistent. Staff will be unaware as to whether or not they are acting within the organisation's risk appetite.
6. To mitigate cyber threats and attacks it is important to:

- document the rules and guidelines around system management, operation and use;
- comply with these documented rules and guidelines.

By following these steps organisations have proactive steps in place to protect their systems, people and customers.

Risk considerations

When providing access to their valuable assets (such as vehicles, machinery and building facilities), organisations expect users to fully understand their terms of use, health and safety considerations, and in some cases the need to complete operator training.

However, the same level of expectation regarding how they interact with valuable systems and data assets is often not well detailed. Typically, the investment in developing, delivering and maintaining a comprehensive suite of IT security policies is minimal, or out of sync with an organisations overall technology spend, which creates a business risk.

The business catalyst for implementing IT security policies should not be an IT related issue or disaster, instead it should be driven from the top of the organisation and based on business impact analysis, risk assessment, and risk mitigation strategies.

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 your customers)
- Loss of data (yours or your customers)
- System unavailability
- Project failure
- Legal or regulatory issues

Business benefits

Developing, delivering and maintaining IT security policies helps an organisation to identify and manage business risks. Having well defined policies that are communicated to staff, and regularly reviewed and updated return the following benefits to the business:

- Provide a security and acceptable use framework
- Help to protect the information systems and information assets
- Enable the successful adoption of new technologies
- Provide a uniform level of control and guidelines
- Communicate IT security and acceptable use policies and guidelines
- Provide a benchmark for monitoring, measuring, and meeting compliance requirements
- Assist with issues relating to the misuse of technology or information
- Meet internal obligations of auditors and risk managers

Stakeholder input

A cross section of stakeholders such as the CIO; IT Manager; and Network and System Administrators should be involved in the development, maintenance, and approval of IT security policies. Input from Human Resources, Information Management, Risk and Governance, and Legal departments is also recommended. Ultimately, it is the Senior Executive and Management Teams who should formally approve the policies.

Typical shortcomings

1. The DIY approach. Writing effective policies that are easy to understand, up-to-date, and contextually correct takes time to perfect. It is therefore a job that's continually put in the too hard basket, or de-prioritised in favour of seemingly more interesting projects.

2. Copying a best practice manual doesn't correlate with how an organisation operates in reality. Policies that do not reflect an organisations' specific business requirements are likely to be disregarded.

3. Not going through a structured engagement and review process. In drafting policy content it is important to take the time to engage with stakeholders to review and customise the policy statements and ensure that they are appropriate for the organisation.

4. Failure to keep policies up to date with changes to operational practices and technology. It's not uncommon for users to identify errors or omissions in outdated policies because no one has been assigned responsibility for their upkeep, or the development of new policy material.

5. There is no launch plan. Presenting the right level of information to senior management for approval, socialising the content with staff and providing supporting resources such as training are key to ensuring that policies are understood, accepted, and ultimately effective.

Ongoing management considerations

Some organisations operate with the reactive mindset, "as long as things are running smoothly" there is no need to worry about documenting policies, procedures and processes.

Other organisations have an unstructured way of managing any IT security policy content that they have in place. Where some policies exist, they often comprise of a few documents that have been published somewhere on the organisation's intranet. They may be out of date, available in hardcopy only, and not readily available to the wider user community. It is not uncommon to find the "ownership", and hence management of IT security policies is inconsistent, fragmented, and low priority.

How does Policy Management as a Service assist?

1 Protocol Policy System (PPS)'s *Policy Management as a Service* solution allows an organisation to develop and deliver a suite of IT security policies in 5 weeks.

2 The policies contained within the solution are tailored for each customer to meet their business requirements, and are mapped to recognised international standards and best practice guidance.

3 Our methodology includes a comprehensive workshop designed to engage stakeholders with the review and tailoring of the content.

4 Once deployed it is crucial to maintain the content. Under the subscription model PPS provide subject matter expertise and ongoing support to ensure the policies, standards, best practice guidance and all other elements are kept up to date.

5 During the delivery process our experts provide advice to customers on a range of factors that will make for a successful launch – e.g., considerations for sign off, how to navigate and use the system, and options for user induction.

What types of organisations use Policy Management as a Service today?

Policy Management as a Service is applicable to any organisation that uses technology to carry out its business. It is cloud based, totally scalable, and no admin or user training is required. The service caters for customers with less than 20 staff through to those with thousands of users. A wide range of customer types use the service including Central and Local Government agencies, and organisations in commercial sectors including Finance, Insurance, Utilities, Not for Profit, Infrastructure, Transport, and Retail.