WHITEPAPER

IMPLEMENTING EFFECTIVE IT SECURITY POLICIES

KAON SecurITy

This whitepaper explains why a robust IT security framework is a necessity in any business environment, and details the steps required to implement a fit for purpose best practice solution.

THE IMPORTANCE OF IT POLICIES

IT systems are a crucial part of most business operations, but too often an organisation's expectations regarding the use and protection of these systems, along with the data they hold are not well detailed.

Typically, the investment in developing and maintaining a comprehensive suite of IT security policies is minimal, or out of sync with an organisation's overall technology spend, and this creates a business risk.

If you've put off implementing IT security policies because of the cost or complexity, or you consider it nothing more than a box-ticking exercise – it's time to think again.

THE BUSINESS BENEFITS OF EFFECTIVE IT POLICIES

Effective, fit for purpose, well maintained IT policies will decrease organisational risk, enabling you to conduct business with greater confidence and peace of mind.

With a growing number of enterprises requiring their third-party suppliers to demonstrate that they have appropriately documented IT practices as a condition of doing business, formalising and implementing policies could help win new customers.

Furthermore, robust IT security policies are a core element of an effective business transformation strategy. They're a key part of a practical digital programme that enables organisations to overhaul their legacy IT systems, improve capabilities, and strengthen their cyber security posture.

The benefits of having well defined policies and procedures based on recognised standards that are communicated to staff, and regularly reviewed and updated, include:

- Providing a suitable framework for protecting IT systems and information assets
- Enabling the successful adoption of new technologies
- Providing a uniform level of control and guidelines
- Streamlining the communication of IT security and acceptable use policies and guidelines
- Assisting with issues relating to the misuse of technology or information
- Enabling a benchmark for monitoring, measuring, and meeting compliance requirements
- Meeting customers' third-party compliance requirements
- Helping meet the internal obligations of auditors and risk managers

KAON SecurITy

THE RISKS OF AN AD HOC APPROACH

The volume of data that organisations collect and store continues to increase. Without deploying a suite of comprehensive IT security policies and procedures, a organisation's employees and contractors do not have clear guidance on what their responsibilities are. Data and system management may be ad hoc and inconsistent, and staff will not know whether or not they are acting within the organisation's risk appetite.

On the other hand, data usage, sharing, and leakage risks can be addressed through the use of documented IT security policies and procedures which take the guess work out of information security.

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

- Misuse of data (yours or your customers)
- Loss of data (yours or your customers)
- Financial repercussions due to remediation requirements
- System unavailability
- Loss of business
- Project failure
- Legal or regulatory issues
- Damage to reputation

CHALLENGES AND PITFALLS TO AVOID

Rather than having senior leadership take ownership of IT security policy development in conjunction with a broad range of stakeholders from across the business, some organisations operate with a reactive mindset: as long as things are running smoothly there is no need to worry about documenting policies, processes and procedures.

Other organisations have an unstructured way of managing the 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. This can lead to a number of mistakes being made:

- Taking a 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 deprioritised in favour of seemingly more interesting projects.
- Copying a best practice manual that doesn't correlate with how an organisation operates in reality. Policies that do not reflect an organisation's specific business requirements are likely to be disregarded.
- Not going through a structured engagement and review process. When 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.

- Failing 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.
- Not having a 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.

THE SOLUTION: POLICY MANAGEMENT AS A SERVICE

To overcome the risks and challenges of implementing an IT policy framework, Protocol Policy Systems developed Policy Management as a Service, a subscription solution that allows an organisation to develop and deliver a framework of IT security policies in under five weeks.

Policy Management as a Service hosts a consistently updated suite of IT policies – including mappings to key standards such as ISO 27002:2022, PCI-DSS v4.0 and ASD (Australian Signals Directorate) Essential 8 – which are uniquely tailored to suit your organisation's environment.

The advantages of deploying Policy Management as a Service include:

- 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.
- The deployment methodology includes a comprehensive workshop designed to engage stakeholders with the review and tailoring of the content.
- Once deployed it is crucial to maintain the content. Under the subscription model, PPS provide ongoing support to ensure the policies, standards and best practice guidance, and all other elements are kept up to date.
- 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.
- We specialise in understanding and keeping up to date with international best practice for IT policies. That means your IT and GRC (governance, risk, compliance) team don't have to – leaving them free to carry on with their core tasks.
- Comprehensive reporting provides visibility of user engagement with the service and content.

Policy Management as a Service is an ideal solution for organisations of any size. Being cloud based, scalable, and with no administrator or user training required, the service is suitable for an organisation with less than 20 staff through to those with thousands of users.

A wide range of customer types use the service including central, local government and organisations in commercial sectors including housing, finance, insurance, not-for-profit, health, utilities, infrastructure, transport, and retail.