Policy Services

Service Description

EthiSEC Pty Limited • PO Box 846, Hornsby, NSW 2077 • T 1300 67 22 75 • ethisec@ethisec.com.au • www.ethisec.com.au

Introduction

Information Security is a discipline that addresses business risk that focuses on business Information and the Information Technology (IT) tools that enable today's businesses. EthiSEC is pleased to offer a Business Policy Services (BPS), we can be engaged to review, develop or extend your organisations Business and Information Technology/Security policies.

The primary focus of the BPS service is to consult with all levels within a business to develop appropriate technology related policies, processes and procedures that underpin an organisation's risk position and business goals.

What is a Security Policy?

A security policy is a framework of living documents that allow an organisation and its management team to communicate, clear, understandable objectives, goals, rules and formal procedures that define the overall security posture and architecture for the organisation.

Why we need policies

We live in a "digital age" where technology enabled business information has become a vital business resource.

This information is supplied by many varied forms of connected technology from network attached computers, phones, faxes and printers and all of these networked devices are accessible 24/7 from anywhere in the world.

While IT has made many business processes faster and simpler the technologies employed have also added new "risks" and complexities to the business environment. These risks come from both internal and external sources and may be intentional or unintentional in nature. Regardless of where they originate all risks pose a threat to the *Availability*, *Integrity* and *Confidentiality* of critical business information and IT resources.

Well written, informed policies are an essential business tool to help manage and mitigate these risks. Policies also provide your business a degree of legal protection. Why? Because by simply developing and using well designed policies you can demonstrate due diligence because you have identified and are managing your organisations risk exposure.

Who needs policies

All businesses need comprehensive, well developed policies. From small one man shows through to multinational companies with hundreds of thousands of employees, they all need policies.

What is a Security Policy

Security policies identify business solutions to threats and communicate those solutions to all concerned. They also detail the what, why where and how as it were, of what is an acceptable use of the network resources.

The foundations of good policies are they:

- Should be easily understood
- Should be realistic and meet business, technological and security needs (i.e. not too restrictive).
- Should be consistent
- Must be supported/endorsed by senior management
- Must be enforceable
- Must be fully documented, distributed and communicated to the

Policy examples

- Privacy Policy
- Electronic mail (email) Policy
- Acceptable use Policy
- Remote Access Policy
- Password Policy

organisation
- Must be flexible and adaptable as 'stuff' changes, often rapidly!
- Must be reviewed regularly - at a minimum annually

Our Approach

Security and specifically security policies in this instance are not a one size fits all proposition. Businesses are different with different needs, resources and risk profiles. EthiSEC's aim is to provide relevant, standards-based system of policy documents that underpin your current business needs. We also aim to develop policies that are flexible enough to grow with your business.

As with all of our services we adopt a top-down approach to developing security polices. The process is initiated with the businesses Management and key stakeholders and works down to the shop floor as required. This approach is adopted to ensure we help you capture your unique requirements to deliver an end-to-end view of *your* business.

Failure to adopt and end-to-end view may result in policies that do not and possibly cannot support your businesses operational requirements. More importantly though failure of a business to understand its business risks, and failure to take appropriate steps to mitigate those risks may have substantial consequences for both the business and its Directors.

How to engage EthiSEC

EthiSEC can be engaged in a number of ways including:

- We may be engaged to lead the development of an organisations Information Security policies.
- We may be engaged on an ad-hoc basis to review or remediate your current policies.
- We may be engaged to help educate and inform your staff on the inherent risks associated with the use of Internet based communications technologies.

Regardless of the engagement model that you choose, to ensure policies maintain their business relevance and effectiveness as a security tool, policies should be reviewed at least once a year. Some businesses find it difficult to allocate time and human resources to do this and value having an independent expert to assist them.

Whatever your type and size of your business, whatever technologies your business employs, whatever skill levels your business has, whatever concerns you may have, EthiSEC has the ability to assist and add value to your business processes.