CMSGu2011-04

NCB

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Information Security Policy

CERT-MU

National Computer Board

Mauritius

Version 1.5

July 2011

Issue No. 4

DISCLAIMER: *This guideline is provided “as is” for informational purposes only. Information in this document, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

Table of Contents

Table of Figures

1.0 Introduction

1.1 Purpose and Scope

The purpose of this document is to provide guidance to users in developing information security policies within their organisations.

1.2 Audience

This document, while generic in nature, provides the background information to understand the development of information security policies. The intended audience for this document includes information security managers, information security professionals, risk analysts, security policy and compliance analysts and all those who are involved in writing security policies for their organisations.

1.3 Document Structure

This document is organised into the following sections:

Section 1 provides a brief overview of the document's content.

Section 2 enlarges on the purpose of an information security policy.

Section 3 presents the basic structure of an information security policy.

Section 4 gives details on the development process of the policy.

Section 5 shows how to introduce the policy to employees.

Section 6 advises on the positive operation of the policy.

Section 7 discusses the policy assessment and review

Section 8 concludes the document.

Section 9 contains a list of references used in drafting this document.

Appendix A includes the template of an information security policy

2.0 Purpose of an Information Security Policy

2.1 Basic Structure of an Information Security Policy

An information security policy should fulfil many purposes. It should:

- Protect people and information
- Set the rules for expected behaviour by users, system administrators, management, and security personnel
- Authorise security personnel to monitor, probe, and investigate
- Define and authorise the consequences of violation
- Define the company consensus baseline position on security
- Help reduce risk
- Help track compliance with regulations and legislation

Information security policies provide a framework for best practice that can be followed by all employees. They help to ensure risk is minimised and that any security incidents are effectively addressed. Information security policies also help in the company's efforts to secure its information assets, and the process of developing these policies will help to define a company's information assets. Information security policy defines the organisation's attitude to information, and announces internally and externally that information is an asset, the property of the organisation, and is to be protected from unauthorised access, modification, disclosure, and destruction.

2.2 Information Security Policy and Regulatory Compliance

In addition to aforementioned purposes, security policies can be useful in ways other than the immediate protection of assets and policing of behaviour. They can be useful compliance tools, showing what the company's status is on best practice issues and that they have controls in place to comply with current and forthcoming legislation and regulations. In today's corporate world it is essential for companies to be able to show compliance with current legislation and to be prepared for forthcoming legislation. Policy can be used to help companies ensure they have the controls in place to work towards compliance by mapping policy statements to legislative requirements. In this way they can provide evidence that their baseline security controls are in line with regulations and legislation. This approach will also give companies an indication based on legal requirements of what they need to protect and to what extent. This will help to ensure that they target security controls only where they are required, a benefit from both a financial and personnel resourcing perspective.

2.3 Information Security Policy as a method for Change

It is also possible to use information security policies to drive forward new company initiatives, with the policy acting as the channel for future projects which move towards better security and general practices. For example, an information security policy stating that a certain type of encryption is required for sensitive information sent by e-mail may (with prior consultation with the appropriate technical experts) help to promote the need to develop such a capacity in the future. The presence of this requirement in policy has made sure the impetus to develop the e-mail encryption project has remained strong.

In short, an information security policy should be a useful tool for protecting the security of the Enterprise, something that all users can turn to in their day-to-day work, as a guide and information source. All too often however, security policies can end up simply on a shelf - little read, used, or even known of by users and disconnected from the rest of company policy and security practice.

2.4 Policies must be Practical

The key to ensuring that your company’s information security policy is useful and useable is to develop a suite of policy documents that match your audience and integrate with existing company policies. Information Security policies must be useable, workable and realistic. In order to achieve this it is essential to involve and get buy-in from major players in policy development and support (such as senior management, audit and legal) as well as from those people who will have to use the policies as part of the daily work (such as subject matter experts, system administrators and end users).

In order to achieve this, one important element is to communicate the importance and usefulness of information security policies to those who have to live by them. Often users seem to think that policy is something that is going to stand in the way of their daily work. An important element of policy development, and to ensure policies are put into practice and not rejected by the users, is to convey the message that policies are useful to users: to provide a framework within which they can work, a reference for best practice and to ensure users comply with legal requirements. Once users realise that policy is something that may actually help them as they perform their work, they are much more likely to be receptive to both helping you develop it and living up to it to ensure compliance. Similarly, once senior management realise that policy is a tool they can leverage to help ensure adherence to legislative requirements and to move forward much needed new initiatives, they are much more likely to be supportive of policy in terms of financial and resourcing.

3.0 Basic Structure of the Security Policy

3.1 Positioning of the Information Security Policy

The system of the Information Security Policy has a hierarchical structure as shown in Figure 1 below. At the top of the pyramid is "the organisation basic concepts of information security," which illustrates how an organisation, as a whole, feels about the measures for information security. The basic concepts are followed by the "basic guidelines (of each department)," "standard of measures (of each department)," and "implementation procedure (of each department)" in this order. The "Information Security Policy" or "the Policy" in these Guidelines refers to the basic guidelines and standard of measures, and does not include the implementation procedure.

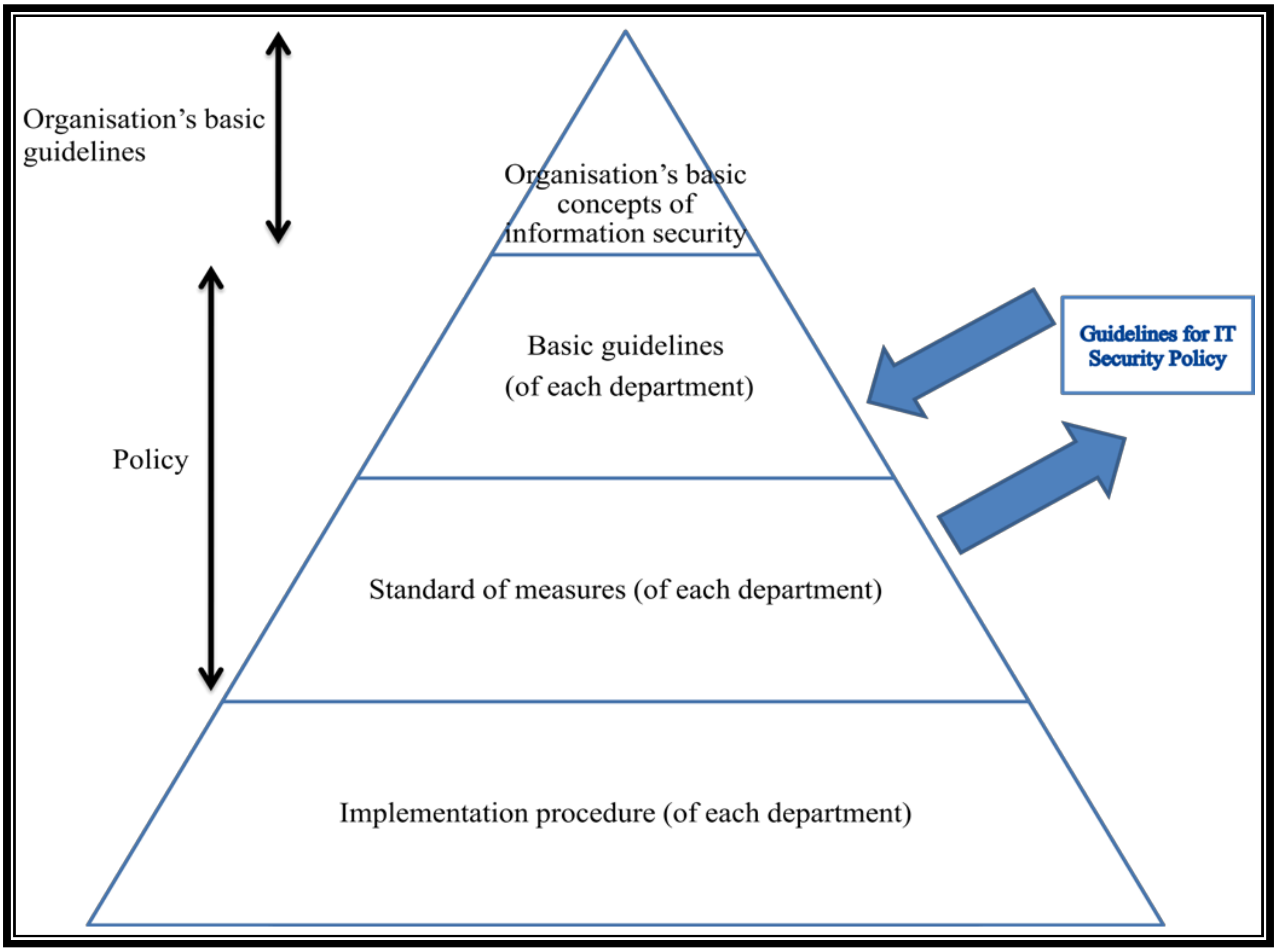
Organisation's basic guidelines
Policy
Organisation's basic concepts of information security
Basic guidelines (of each department)
Standard of measures (of each department)
Implementation procedure (of each department)
Guidelines for IT Security Policy

Figure 1 Basic Structure of an Information Security Policy

3.2 Policy Types

3.2.1 Policy Hierarchy

The diagram below outlines a hierarchical policy structure that enables all policy audiences to be addressed efficiently. This is a template for a policy hierarchy and can be customised to suit the requirements of any company:

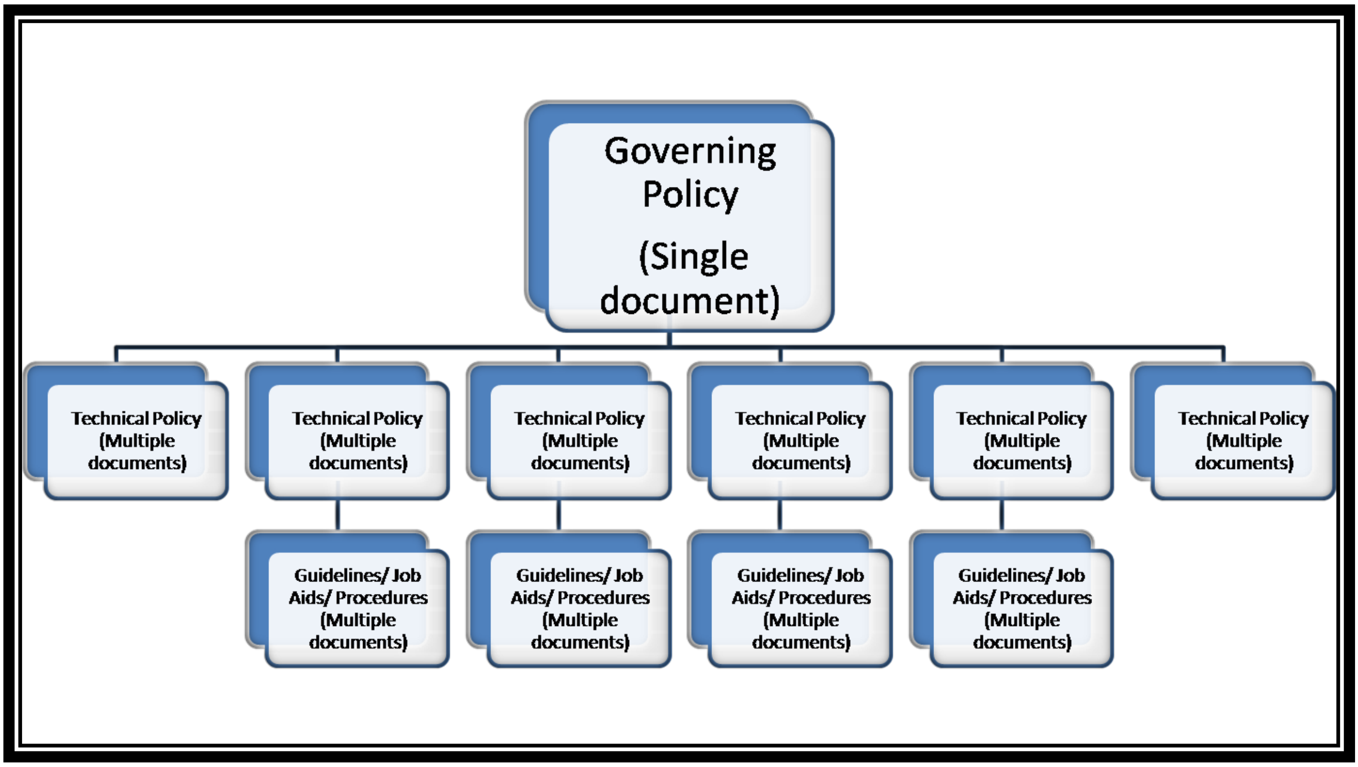
Governing Policy (Single document)
Technical Policy (Multiple documents)
Technical Policy (Multiple documents)
Technical Policy (Multiple documents)
Technical Policy (Multiple documents)
Technical Policy (Multiple documents)
Technical Policy (Multiple documents)
Guidelines/ Job Aids/ Procedures (Multiple documents)
Guidelines/ Job Aids/ Procedures (Multiple documents)
Guidelines/ Job Aids/ Procedures (Multiple documents)
Guidelines/ Job Aids/ Procedures (Multiple documents)

Figure 2 Policy Hierarchy

The diagram above shows the hierarchy for a large company where policy development has been on track for several years. For smaller companies or for those just starting to develop policy, it is possible to use this basic framework, but it is advisable to initially have a smaller number of technical policies and possibly no guidelines or job aids in the early phases. Rather than trying to develop a large hierarchy all at once, it is more realistic to develop a governing policy and a small number of technical policies initially, and then increase the number of policies and supporting documents, as well as the complexity of the policies as you move forward. In large companies there will be several audiences for your policy, and you will want to cover many different topics on different levels. For this reason, a suite of policy documents rather than a single policy document works better in a large corporate environment. The hierarchical structure of the suite of information security policy documents reflects the hierarchical structure of roles in a large company. The proposed scheme provides for all levels of audience and for all topics by using two policy types supported by procedural documents:

- Governing Policy
- Technical Policy

3.2.2 Governing Policy

Governing policy should cover information security concepts at a high level, define these concepts, describe why they are important, and detail your company's position. Governing policy will be read by managers and end users. By default it will also be read by technical custodians (particularly security technical custodians) because they are also end users. All these groups will use the policy to gain a sense of the company's overall information security policy viewpoint. This can be used to inform their information security-related interaction with business units throughout the company. Governing policy should be closely aligned with existing and future Human Resources and other company policies, particularly any which mention security related issues such as e-mail or computer use, etc. The governing policy document will be on the same level as these company-wide policies. Governing policy is supported by the technical policies which cover topics in more detail and add to these topics be dealing with them for every relevant technology.

Covering some topics at the governing policy level may help avoid the need for a detailed technical policy on these issues. For example, stating the company's governing password policy means that details of specific password controls can be covered for each operating system or application in the relevant technical policy, rather than requiring a technical policy on password controls for all systems. This may not be the case for a smaller company, where fewer systems/applications are used and where a single technical password policy would therefore be sufficient. For a larger company however, the former method provides a more efficient process for users to follow because they will have to reference fewer documents. Simplifying this process means more users will comply with the policy, thereby improving security. In terms of detail level, governing policy should address the "what" in terms of information security policy.

3.2.3 Technical Policies

Technical policies will be used by technical custodians as they carry out their security responsibilities for the system they work with. They will be more detailed than governing policy and will be system or issue specific, e.g., a technical physical security policy. Technical policies will cover many of the same topics as governing policy, as well as some additional topics specific to the overall technical topic. They are the instruction manual for how an operating system or a network device should be secured. They describe what must be done, but not how to do it. This is reserved for procedural documents which are the next detail level down from governing and technical policy. In terms of detail level, technical policy should address the “what” (in more detail), “who”, “when”, and “where” in terms of information security policy.

4.0 Information Security Policy Development Process

4.1 Policy Development Team

It is important to determine who is going to be involved in the actual development phase of policy at an early stage. The group who develops the policy should ideally also be the group who will own and enforce the policy in the long-term; this is likely to be the information security department. The overall composition of the policy development team will vary according to the policy document being developed, but the following is a list of individuals or groups who may be involved.

4.1.1 Primary Involvement

- **Information Security Team**

  A team or part of a team from this group should be assigned the overall responsibility for developing the policy documents. Overall control may be given to one person with others in a supporting role. This team will guide each policy document through development and revision and should subsequently be available to answer questions and consult on the policy.

- **Technical Writer(s)**

  Your company or security department may already have a technical writer on staff who can assist in writing security policies. Even if they are not able to take primary responsibility for the information security policy project, an in-house technical writer can be a valuable resource to help with planning your policy project, determining an appropriate style and formatting structure for your documents, and editing and proof-reading your policy drafts.

4.2.2 Secondary Involvement

The following groups may (and in some cases, should) have input during the development of the policy in reviewing and/or approval roles.

- **Technical Personnel**

  In addition to staff on the security team, you may need to call upon technical staff who have specific security and/or technical knowledge in the area about which you are writing. They will be familiar with the day-to-day use of the technology or system for which you are writing the policy and you can work with them to balance what is good security with what is feasible within your company.

- **Legal Counsel**

  Your Legal department should review the policy documents once they are complete. They will be able to provide advice on current relevant legislation such as the Mauritian Data Protection Act 2004 that requires certain types of information to be protected in specific ways, as well as on other legal issues. The Legal department should also have input into the policy development process in terms of letting the policy development team know about forthcoming legislative requirements and helping to interpret these for the team.

- **Human Resources**

  The Human Resources department may need to review and/or approve your policy depending on how you have determined that your policy will relate to existing company policies. Where your policy touches on topics covered by existing HR policy, e.g., e-mail usage, physical security, you must make sure that both sets of policy say the same thing.

- **Audit and Compliance**

  The Internal Audit department in your company is likely to be involved in monitoring company-wide compliance with the policy once it is enforced. It is therefore useful if they are involved in the development and review processes for policy to ensure that it is enforceable in terms of their procedures and current best practice. If there are other compliance groups additional to the main internal audit department, these groups should also be consulted as needed.

- **User Groups**

  During revision of policy documents, it can be useful to work with users to determine how successful the current policy is, and thereby determine how the policy may need to be changed to make it more useable for your target audiences. Issues such as the style, layout, and wording of your policy documents may seem minor issues compared to their content, but remember that if your documents are hard to understand; users may not read them fully or may fail to understand them correctly, thereby needlessly risking security compromise.

4.2 Development Approach

4.2.1 Development Process Maturity

The major consideration behind any company's policy development process will be the level of process maturity. It is important that companies (especially larger ones) do not aim too high initially and try to develop a comprehensive and complex policy program straight away. This is not likely to be successful for a number of reasons including lack of management buy-in, unprepared company culture and resources and other requirements not in place. In this situation it is advisable to start off small, perhaps developing checklist–style policies initially and only a skeleton policy framework with essential policies developed first. As the process grows in maturity, companies will be able to develop the full range of policies with more detail included in each as well as accompanying procedural documentation as needed. Education, awareness and communication processes will also grow in maturity to cope with promoting an ever-growing range of policies. This should match the growing corporate strength of the policies themselves. The corporate culture will start to appreciate that the policies must be followed and may actually start to use them to push through much needed changes throughout the company.

4.2.2 Top-Down versus Bottom-Up

There are many starting points for developing policy. New or forthcoming legislation can often be a powerful impetus to develop policy, as can recent security incidents or enthusiastic administrators recently returned from the latest training course. All these provide great inputs to policy but the key is to be balanced. Relying solely on the 'top-down' approach of using only legislation, regulations and best practice to write your policy will leave you with unrealistic, artificial policy that will not be workable in the real world. Similarly, relying only on a 'bottom-up' method based only on system administrator knowledge can result in policy that is too specific to a given environment (perhaps just one part of a large company), possibly based too much on local current practice or on the latest training suggestions, making it too unrealistic. The best policy will come from a combination of these approaches, both top-down and bottom-up. In order to achieve this it is something that must be considered from the beginning and must be reflected in the diversity of areas involved in policy development and the types of review the policy undergoes. This balanced approach is likely to result in a more mature policy development process. It can work for both small companies (where there is little space between top and bottom) and big companies where the breadth of knowledge is needed to ensure a realistic and workable resulting policy.

4.2.3 Current Practice versus Preferred Future

Policy development must also take into account to what extent the policy should reflect current practice versus preferred future. Writing a policy that reflects only precisely what is done today may be out-of-date even by the time it is published, while a policy that includes controls which cannot yet be feasibly implemented may be impossible to comply with for technical reasons and may therefore be ignored as unrealistic and unworkable. It is important that this is discussed at an early stage as if it is not discussed and the policy develops too far towards the unworkable, preferred future model, this may only then show up at the policy gap identification stage, when a lot of time and effort will then have been wasted developing something which is of little value. The best policy strikes a balance between current practice and preferred future and this is what the policy development team should aim for.

4.2.4 All Threat Types Consideration

Finally when considering what should be included in an initial draft, make sure to consider all the types of threats your company faces. While those from malicious external attackers in the form of viruses and worms attract much media attention and accordingly deserve to be considered when writing policy, other considerations that are at least as important include natural disasters, disgruntled current and former employees and ignorance leading to accidental security exposures. Policies should consist of controls to combat all these threat types.

5.0 Introduction of the Policy to Employees

The policy should be thoroughly known to the related persons before its operation is started so that it can be successfully implemented.

5.1 Audience Groups

Your audience is of course all your company employees, but this group can be divided into audience sub-categories, with the members of each sub-category likely to look for different things from information security policy. The main audiences groups are:

- Management – all levels
- Technical Staff – systems administrators, etc
- End Users

All users will fall into at least one category (end-user) and some will fall into two or even all three.

5.2 Implementation Procedure

The implementation procedure provides how the contents of the policy should be put into operation for actual work or in the information system. The implementation procedure is equivalent to a manual that defines what each person who should observe the policy must do to maintain information security according to the information handled and the work to be done. Therefore, the implementation procedure has to be determined for individual cases when necessary, according to the actual working environment. It should be provided that the existing regulations could be used where applicable. It shall be allowed that the implementation procedure be set up, updated, and abolished by the relevant departments without approval from the Information Security Committee.

5.3 Conformity to the Policy

The information security officer would verify that the implementation procedure and the actual implementation conform to the policy before it is put into operation. The Committee collects and analyses information about conformity to the policy and provides appropriate advice or actions for the operation of the policy in advance. The officer in charge of information security should verify that the physical, human, and technical information security measures, as well as the emergency action plan and the implementation procedure introduced for all information assets s/he is responsible for, conform to the Policy.

5.4 Distribution and Briefing

The Information Security Committee distributes prints of the policy or holds briefing about it to make it known to related personnel. Each department will be responsible for making the implementation procedure known to related personnel. It is desirable that the necessary part of the policy is made known to outside recipients to have them agree to the conformance to the policy. The implementation procedure is confidential. The related persons, including outside recipients, should handle the procedure under strict control.

6.0 Positive Operation of the Policy

Establishment of organisations or systems, monitoring, actions taken at the time of intrusion, and other measures, should be provided for positive operation of the policy.

6.1 Operation management

Persons in charge of information security in information management sections and the departments and bureaus should make sure that physical, human and technical information security measures are implemented appropriately under the Information Security Committee.

6.2 Disciplinary Actions

If a violation of the measures that could cause a serious problem for information security is found, actions should be taken in accordance with a plan of emergency measures. These actions must be managed with tight control ready for use for the assessment or review of the policy because they can serve, not only as proof of violation, but as materials for measuring the practicability of the policy.

7.0 Policy Assessment and Review

Regular assessment and review of the standard of measures are important. It should be done in consideration of the evaluation of the policy and the information security measure, changes of the information system and emergence of new threats. The assessment and review should be done under the Information Security Committee to keep the policy practical and keep the information security level high.

7.1 Auditing

If an external auditing organisation is used, sufficient consideration should be given to its credit. It should capture weak points of the information system subject to the audit.

7.2 Policy Update

Updating the policy for the first time after its introduction requires special consideration. Since differences between the policy and the reality have to be considered, it is desirable to capture the actual states by canvassing opinions from the sections concerned, or by other means. Updating the policy should begin with risk analysis to make it practical. Information about new methods of attacking systems should be collected for reference purposes for updating the policy. The updated policy has to be redistributed and applied. This requires as much trouble as that required when the policy was introduced. Efforts should be made to seek efficient methods.

8.0 Conclusion

Policy is both the starting point and the standard for information security in any organisation. It provides evidence of the organisation's position on security and provides a living tool for every employee to help build and maintain that level of security. It is therefore essential that an information security policy is accurate, comprehensive, and useable. It can be a tedious task to produce policy that lives up to this standard. Assessing policy audiences, topics, and methods using the processes described in this paper will help to ensure that your policy documents are as efficient and useable as possible. In turn, this will help ensure that your efforts to raise the standard of security in your company are worthwhile.

9.0 References

- Japanese Government: Guidelines for IT Security Policy
- SANS Institute InfoSec Reading Room: Developing a Security Policy - Overcoming Those Hurdles
- SANS Institute InfoSec Reading Room: Information Security Policy - A Development Guide for Large and Small Companies
- SANS Institute InfoSec Reading Room: Security Policy: What it is and Why - The Basics
- SANS Institute InfoSec Reading Room: Security Policies - Where to Begin

Appendix

Policy Document Outline

In addition to the policy statements that will form the main body of your policy documents each policy should include the following sections:

Overview

This section should introduce the policy by name and locate it within the hierarchy of other existing information security and company policy documents.

Purpose

This should state the main goals of the policy. It will explain the reason for the policy and help readers understand how the policy should be used. Legal and compliance issues should also be mentioned in here. Statements on any specific legislation the policy is designed to adhere to should be included here.

Scope

The scope is a statement of the infrastructure and information systems to which the policy applies, and the people who are stakeholders in it. Stakeholders would typically include anyone who is a user of the information or systems covered by the policy.

Roles and Responsibilities (Optional if policy is generic)

This is a statement of the structures through which the responsibilities for policy implementation are delegated throughout the company. Job roles may be specified in this section, e.g., Database Administrators (DBAs), Technical Custodians, Field Office employees, etc.

Enforcement

This section details to what extent breaking policy is considered a violation (e.g., it is HR-related and therefore related to an employee’s contract, or is it an information security department matter?) This section should also detail how violations should be reported, who to and what actions should be taken in the event of a violation. It should also include information on what sanctions will be carried out resulting from a violation (for example, verbal or written warnings, termination of contracts etc).

Policy Update

This section defines who is responsible for making updates and revisions to the policy and how often these will take place. It may be useful to include a reference to the document as a "living document" which can be updated as determined by those responsible for updates and revisions. This will ensure that any ad hoc revisions are accounted for as well as scheduled updates. Information should also be included detailing where the policy will be published and how employees can access it.

Contact information (Optional if policy is for internal use)

Details of who should be contacted in connection with policy. A group or mailbox rather than an individual is preferable here as these are less likely to change.

Definitions/Glossary (Optional)

Define any terms that may be unfamiliar to the reader. The necessity for this will depend on the audience, e.g., the readership of a technical policy for Linux are likely to already be familiar with the Linux technical terms, therefore it will not be necessary to spell these out. The cryptography section of the user policy however may include terms with which readers are not familiar and these should be defined in footnotes or a glossary to aid comprehension.

Acronyms (Optional)

A separate section spelling out acronyms may be required where there are a large number or where the document is long or complex. For shorter documents, acronyms may instead be spelt out in the body of the document.