META Security Group Information Security Policy Framework

Best Practices For Security Policy in the Internet and e-Commerce Age

By Malcolm E. Palmer
Craig Robinson
Jody Patilla
Edward P. Moser

Copyright Notice

META Security Group
20464-A Chartwell Center Drive, Charlotte NC 28236-6862
704-895-0837 fax: 704-895-8165
World Wide Web site at http://www.metasecuritygroup.com

Printed in the United States of America.

Warning and Disclaimer

Table of Contents

Introduction

This research report from META Security Group*, META Security Group Information Security Policy Framework*, provides a best practices policy framework that organizations can reference and leverage to assess, improve, or develop new Information Security policy. The insights provided in this report are derived from the considerable "real world" experience gained by META Security Group in developing and assessing Information Security policies, standards, guidelines, and procedures.

Audience

The audience for this report is primarily members of Information Security teams. In addition, this report can be useful to executive management and business unit owners to enhance communication within the organization and provide a common understanding of the foundations required for a more effective Information Security policy framework.

This report assumes a certain level of understanding of risk management and Information Security policy frameworks, and a basic, but not necessarily an in-depth comprehension of Internet technologies.

Key Terms

These fundamental and key terms used in this report are defined below.

Asset Value: The worth of the assets that organizations are trying to protect.

Charter: The authoritative mission statement for the policy framework. It establishes how to support critical business and operational objectives. The charter outlines key program management issues, such as policy enforcement and management responsibility.

Framework Elements: The charter, policies, standards, guidelines, and procedures.

Gap Analysis: The process of comparing the current state of security against best practices or the desired future state of security to uncover differences, deficiencies, or gaps. This process is used by many consulting organizations to identify areas for improvement.

Policy: The broad rules for ensuring the protection of information assets, and for implementing a security strategy or program. Generally brief in length, policies are independent of particular technologies and specific solutions.

Policy Framework: The hierarchy of security policies, standards, and procedures. Provides the overall foundation for an effective Information Security Program.

Procedures: Specific, step-by-step advice and tactics on how to implement the various standards.

Risk: The likelihood of loss, damage, or injury. Risk is present if a threat can exploit an actual vulnerability to adversely impact a valued asset.

Risk Management: The identification, assessment and appropriate mitigation of vulnerabilities and threats that can adversely impact an organization's information or data assets.

Standard: The acceptable level of security for a specific policy area. Standards may be technology- or solution specific, and provide more measurable criteria for satisfying the high-level objectives defined in the policies.

Threats: The activities or actions that could exploit the vulnerabilities in an organization and place information assets at risk.

Vulnerabilities: The holes and weaknesses in information systems and procedures that intruders can exploit.

Premise

An Information Security policy framework provides an organization with a concise yet high-level and comprehensive strategy to shape its tactical security solutions in relation to business objectives. Moreover, it clearly defines the value of information assets, represents organization-wide priorities, and definitively states the underlying business requirements and assumptions that drive security activities. By going through the process of developing a relevant, usable policy framework, an organization can make the hard decisions on the Information Security Program up front, and make implementation of the rest of the program that much easier. In addition, an organization that regularly reviews and assesses its current policy implementation can identify key missing and ineffective elements within its Information Security Program.

Purpose

The goal of this paper is to outline a detailed Information Security Policy Framework that addresses the shortfalls associated with other policy frameworks and implementations, as well as serves as a best practices baseline reference model for policy framework assessment, gap analysis, and development efforts.

Organization

The remaining portion of this Introduction section discusses the role and importance of Information Security policy in the "open" computing era, as well as the shortfalls and problematic attributes of existing policy frameworks and implementations.

The META Security Group Information Security Policy Framework section provides an overview of the process used to develop the META Security Group Information Security Policy Framework. The Framework Charter and policies are discussed in detail and samples are provided. In addition, the associated standards are outlined.

The Practical Use of the Framework section discusses how organizations can use the Framework to meet their specific needs.

The Practical Issues section discusses specific issues that organizations may confront when using the Framework as a best practices baseline reference.

Appendix A combines the sample Information Security Program Charter and sample policies provided in this document.

Appendix B provides a sample policy interpretation document for wireless access.

Appendix C provides an overview of the benefits of leveraging Web-based, Intranet methods to facilitate policy distribution within an organization.

Background

In recent years, organizations have faced the challenge of a major computing paradigm shift from proprietary networks and systems architectures to "open" systems with distributed, heterogeneous servers and clients. Prior to the emergence of the "open" computing era, data was stored and managed on mainframes and centralized clusters of smaller systems. Strong host-based controls provided significant assurance that information assets were protected from unauthorized access, disclosure, or modification. However, the shift to internal and Internet-based TCP/IP networks, as well as to distributed computing based on desktop PCs or remotely-connected laptops, have reduced the effectiveness of traditional controls.

In addition, the rapid growth of e-Commerce and the Internet has coincided with the trend toward the "virtual corporation," where the lines between businesses and their customers, suppliers, partners and agents are increasingly blurred. The currency of the new digital economy is information and intellectual capital, neither of which has value unless it is shared among authorized entities. Companies are not only making information available outside their own networks, they are allowing outsiders to view or update information on their internal networks. The distributed computing and Internet environments may increase an

organization's efficiency and competitive position in the new economy and online marketplace. However, due to the nature of these "open" computing environments, the risks are greater. Participating in the e-Commerce marketplace requires new security approaches for access controls and data protection. The enormous increase in data sharing means a concurrent need for intelligent regulation of information. In such a milieu, the need for well-defined, carefully considered policy is greater than ever, and in fact may be a prerequisite for doing business.

Many organizations initiating electronic business efforts and leveraging the Internet are finding that their existing policies are either outdated, or have been developed piecemeal over time. In other words, these organizations do not have a coherent security strategy that accurately reflects their current and evolving business needs. Data from the 1999 *Information Week* Research Global Information Security Survey of 2,700 security professionals worldwide reflected this situation (Figure 1).

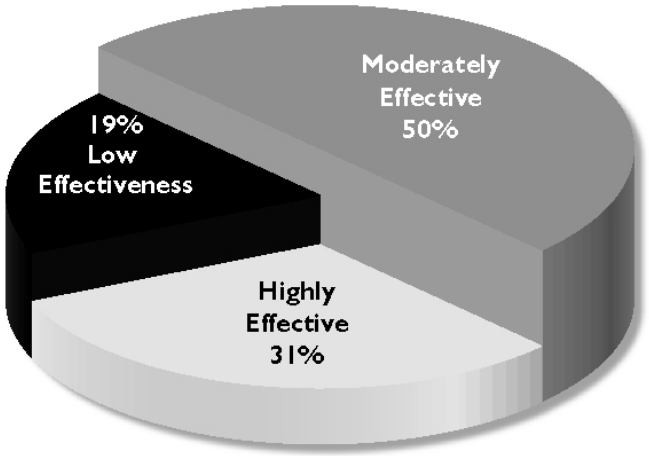

Figure 1: Reported effectiveness of current Information Security policy

The survey found that 19 percent of respondents had ineffective or no security policy. 69 percent believed that their policies did not strongly match business objectives. Only 31 percent described their policies as highly effective.

In addition, the *Information Week* survey found that security policies are rarely reviewed on a regular basis (Figure 2).

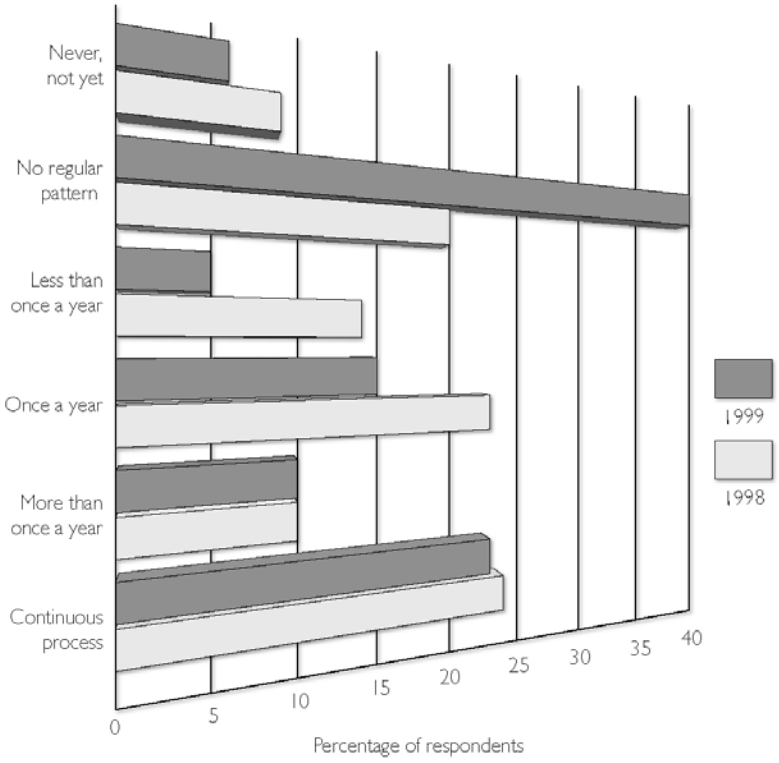

Figure 2: Reported frequency of reviewing Information Security policy

More specifically, 40 percent of the respondents had no regular agenda for reviewing their security policies, 15 percent did so only once a year, and 6 percent never did. Only 10 percent of survey participants undertook the review process more than once a year, and only 24 percent continuously reviewed their security policies.

To further understand why organizations considered their existing policies ineffective and failed to regularly review them, METASES reviewed numerous policy frameworks and implementations. These policy frameworks and implementations consistently exhibited shortfalls and problematic attributes in the following areas:

- **Completeness:** META Security Group reviewed many existing policy framework models where a clear finish line could not be established. These policy frameworks were based on a challenge model where the completeness of the work was not subject to a formal proof. In other words, comprehensiveness and coverage were typically only tested by a challenge such as, "We'll see if you can find any holes in what we came up with." The challenge model could not demonstrate beyond a doubt the completeness of the framework.

- **Cross-Threaded Definitions:** The definitions for policy and related elements such as standards, procedure, guidelines, and processes tended to have many shades of interpretation. Detailed, step-by-step technical standards and procedures were often referred to as policies. Sometimes, various framework elements were used interchangeably. Other times, they were used to convey different things, but were not defined well enough to show how each piece differed, where it fit in the picture, and why it was needed.

- **Traceability**: Most organizations agree that the policy used to frame Information Security hinges on the organization's business or mission, rather than the other way around. However, with the existing policy frameworks and implementations, organizations struggled to provide a direct line of logic between top-level policy and other framework elements to business objectives and needs.

METASES recognizes the need for a comprehensive and practical policy framework that addressed these issues. More specifically, organizations require a policy framework that is well-structured, well-written, and easily distributed, and communicated throughout the organization. Such a framework is outlined in the pages that follow.

META Security Group Information Security Policy Framework

Framework Development

For over a year, META Security Group has been working to develop the META Security Group Information Security Policy Framework™. Figure 3 illustrates the process used by META Security Group to develop the framework.

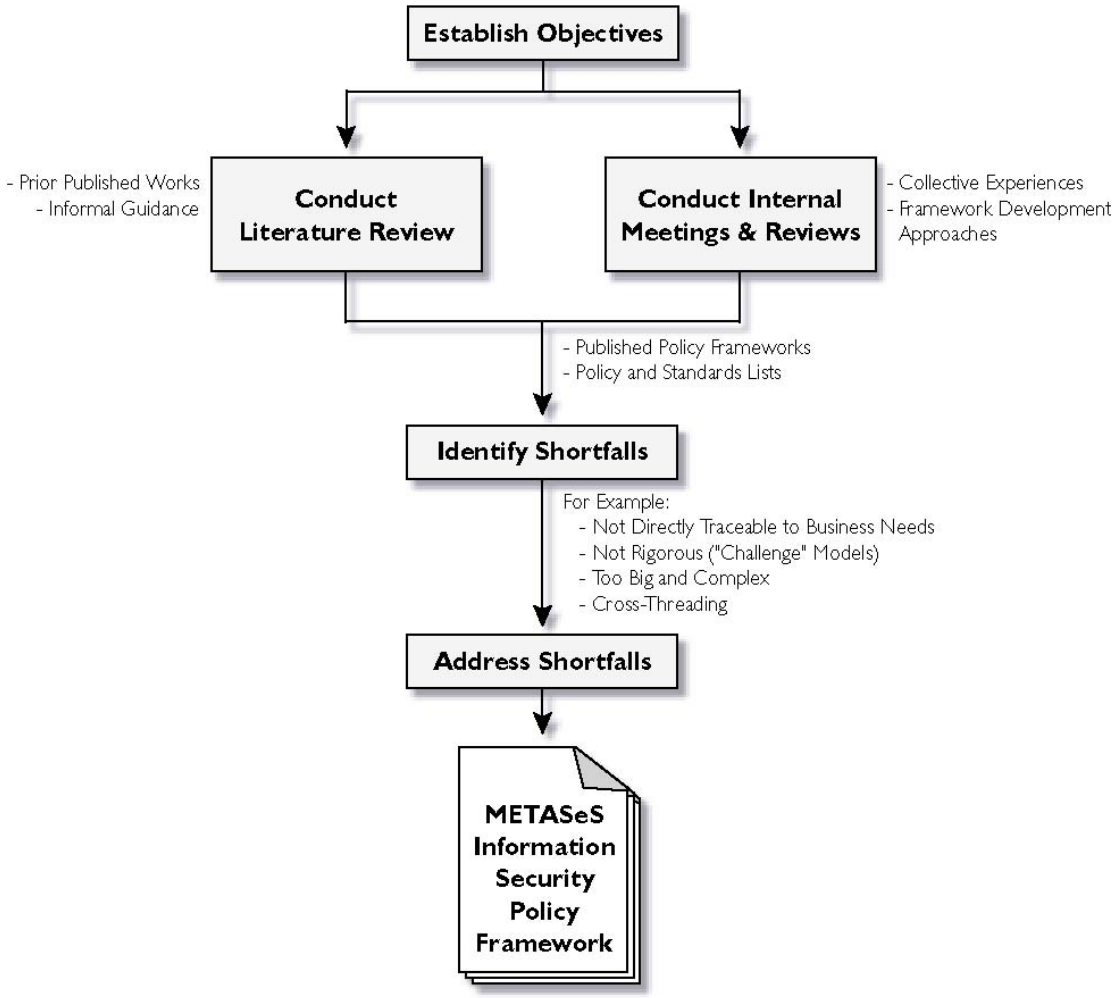

Figure 3: Process for developing the Framework

META Security Group started by defining specific objectives and goals. The initial goals simply involved developing a best practice security policy reference model that would be used to:

- Assess current Information Security policies and perform a *gap analysis* against our "best practice" reference model to highlight necessary improvements.

- Provide a baseline reference model that organizations could use and customize to address specific needs.

However, as the effort progressed, the scope was broadened to developing a *policy framework*. The policy framework would cover not only policy itself, but also address policy-related components such as standards, guidelines and procedures. Thus, META Security Group decided to develop an Information Security Policy Framework that was traceable back to key Information Security tenets and an organization's business or mission goals.

Having defined the specific objectives, META Security Group conducted an exhaustive review of literature in the policy area. META Security Group collectively identified and reviewed an extensive amount of materials on the topic, including research papers from government and commercial sources, published commentary on the Internet, and various books. Fortunately, there were several very talented security policy pioneers such as Thomas R. Peltier, Charles Cresson Woods, and Donn Parker who paved the way in this well-documented area. Moreover, META Security Group recognized that a substantial amount of Information Security policy expertise existed internally within META Security Group itself. Our senior executives and consultants have "real world" Information Security policy and implementation experience derived from decades of related consulting projects and work experience. META Security Group conducted numerous multi-day sessions to leverage the existing materials and internal body of knowledge to formulate an initial policy framework, as well as to identify and address any shortfalls.

Further, this initial policy framework was battle-tested in the "real world." META Security Group distributed the framework to its consulting team, who presented it to numerous clients and leveraged it on several consulting projects. The "real world" feedback was reviewed and incorporated to produce the METASES Information Security Policy Framework.

Framework Concepts

The numerous multi-day sessions and "real world" feedback yielded many of the unique concepts for the META Security Group Information Security Policy Framework. The Framework incorporates five comprehensive concepts that not only differentiate it from other policy frameworks and implementations, but also address several of their shortfalls, including:

- Risk Management Basis
- Hierarchical Policy Structure
- Guideline Definition
- Threat and Vulnerability Policies
- Policy Interpretation

Concept 1: Risk Management Basis

The META Security Group Information Security Policy Framework outlines several policy areas based on risk management objectives that trace back to specific business requirements. Risk is a function of threat, vulnerability, and asset value; it only exists if a threat can exploit an actual vulnerability, and then go on to adversely impact a valued asset. Moreover, it is important to understand that risk can never be completely eliminated; it can only be managed through the application of security measures. An assessment of risks should allow an organization to balance the exposure of valued assets to risks against the cost of risk prevention (Figure 4).

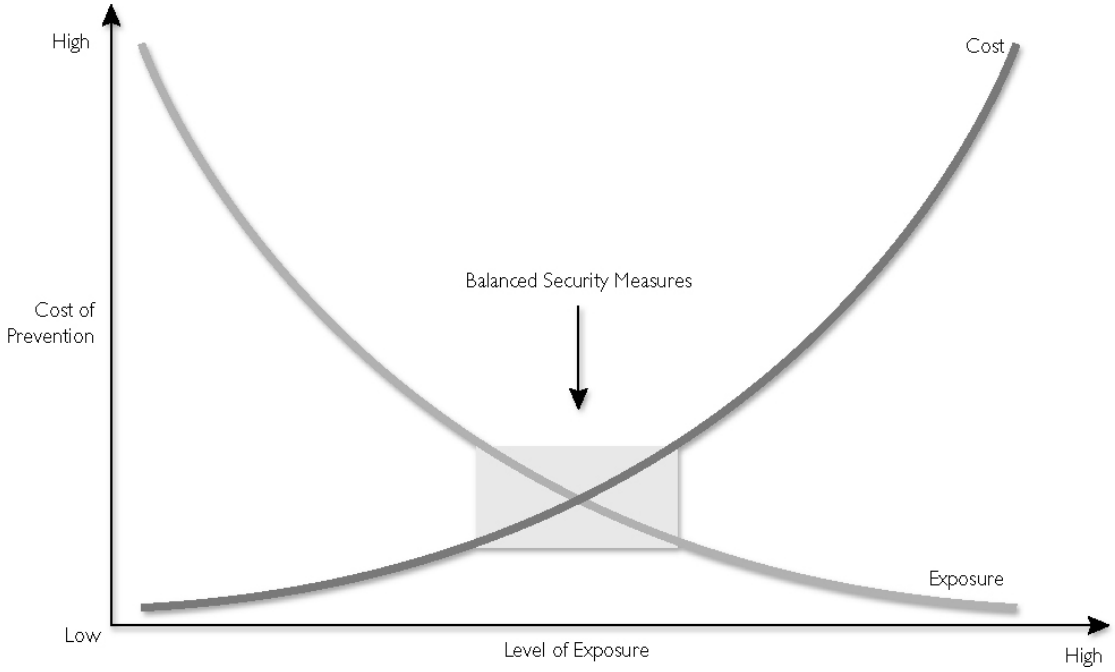

Figure 4: Balancing cost of risk prevention vs. exposure

The risk management approach to Information Security involves identifying, assessing and appropriately mitigating vulnerabilities and threats that can adversely impact the information assets of the organization. As illustrated in the Figure 5, the policy areas and resulting functions relate directly to traceable risk management objectives.

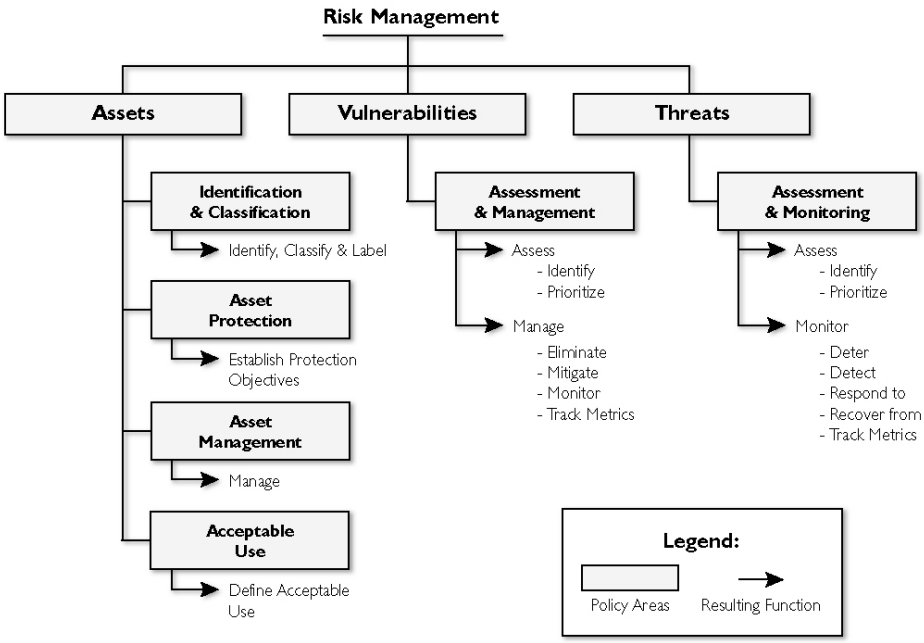

Figure 5: Link between assets, vulnerabilities, and threats and resulting functions

The appropriate and cost-effective mitigation of risk requires that an organization address security objectives and costs in tandem with business and operational goals.

Concept 2: Hierarchal Policy Structure

The META Security Group Information Security Policy Framework uses a hierarchical policy structure to directly link the policies with the risk management strategy and in turn, with other framework elements such as standards, guidelines, and procedures. Figure 6 illustrates the hierarchical nature of the Policy Framework and the relationships among framework elements.

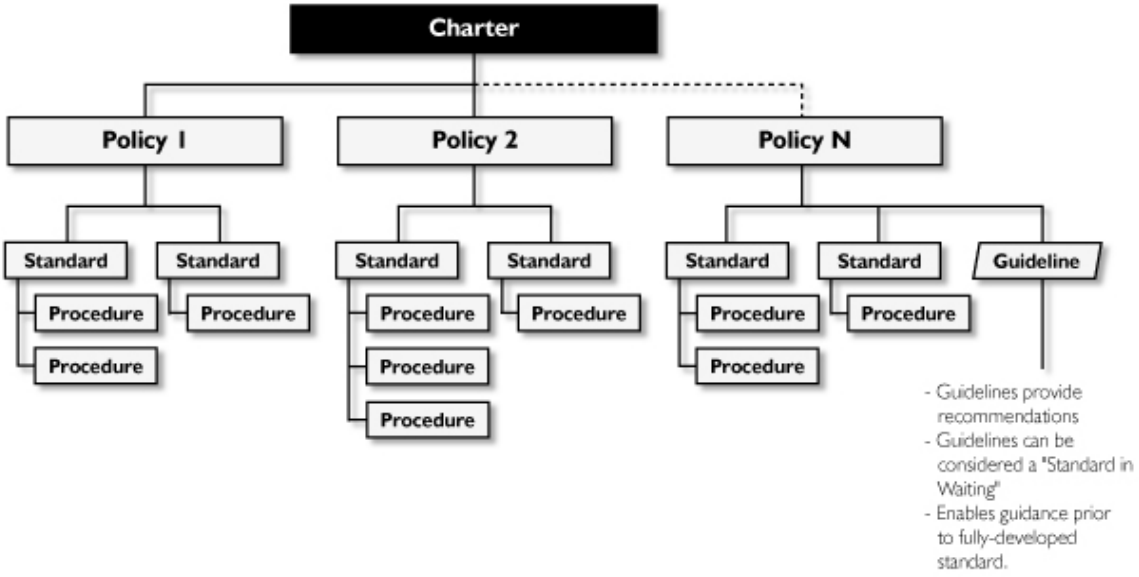

Figure 6. A traceable, hierarchical set of policy guidance documents

As shown in Figure 6, the Policy Framework consists of a hierarchical structure that includes:

- An Information Security Charter at the top of the hierarchy that empowers all activity within the Information Security Program.
- Policies that further define the Information Security objectives in a number of topical areas. For example, proper identification and authentication are required.
- Standards that provide more measurable ("auditable") guidance in each policy area. For example, a standard might specify that usernames must be unique and passwords must contain a minimum of six characters with at least one non-alphabetical character.
- Procedures that describe how to implement the standards. For example, a procedure might specify that authorized personnel will follow certain steps using the password utility to properly configure the minimum password length.

This hierarchical structure ensures that the elements at lower levels in the Framework are referentially associated with the risk management strategy and traceable back to the business objectives.

Concept 3: Guideline Definition

The META Security Group Information Security Policy Framework, as illustrated in Figure 6, uses guidelines to enable initial policy guidance prior to the emergence of fully developed standards and procedures. In earlier policy frameworks and implementations, the definitions of a guideline and standard are often used interchangeably. The META Security Group

Information Security Policy Framework presents a clear distinction by defining a guideline as a "standard in waiting," not as another level or tier in the policy framework hierarchy.

Many organizations require the flexibility to address the risks associated with emerging and less distinct technologies in a timely and focused manner. Guidelines provide this flexibility by allowing an organization to produce and distribute policy guidance on a local or enterprise-wide level in the absence of formal standards and procedures. For example, during the emergence of electronic mail, an organization could have defined an Electronic Mail Guideline prior to developing a complete and thorough set of standards and procedures for reducing the risk of the new technology.

Concept 4: Threat and Vulnerability Policies

The META Security Group Information Security Policy Framework explicitly addresses vulnerability and threat at the policy level. Most policy frameworks and documents do not regard vulnerability and threat as strategic policy topics. In other policy frameworks, vulnerabilities and threats are addressed at the standards level, or not at all. However, the META Security Group Information Security Policy Framework outlines policies for both vulnerabilities and threats since they are essential components of the risk management approach on which the Framework is based.

Concept 5: Policy Interpretation

The META Security Group Information Security Policy Framework introduces policy interpretation as a vehicle to apply existing policy guidance to new Information Technology and Information Security topics. The Framework is comprehensive in its coverage and requires minimal changes to top-level policy areas. The approach of other policy frameworks and implementations involves producing a new top-level policy area for each fundamentally new application of technology. Eventually, this leads to the development of a complex, ad hoc and cross-threaded policy framework. As illustrated in Figure 7, META Security Group avoids a similar outcome through the use of policy interpretation for target audiences (for example, administrators, developers, end users, etc.) or technologies (for example, wireless, hand-held computing devices, etc.)

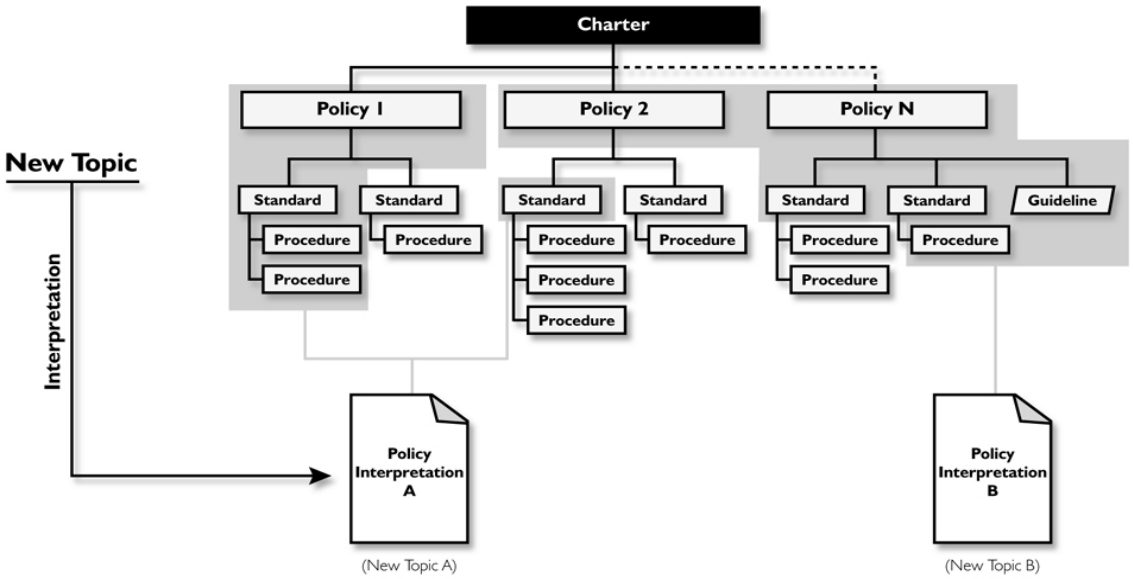

Figure 7: Policy interpretation

For example, wireless technologies are emerging as viable alternatives for periodic network access. Within the context of the META Security Group Information Security Policy Framework, an organization would produce a Wireless Access Policy Interpretation document. This document would concisely reference existing policy guidance and provide the basis for development of lower-level standards and procedures that apply to wireless technology.

More specifically, the Wireless Access Policy Interpretation document would simply reference the Framework's policies, as appropriate, and specifically interpret how they apply to the new technology (see Appendix B).

In general terms, the policy interpretation document should include:

- Introduction: Describes the new technology (for example, potential uses, high-level risks, etc.) and states the purpose of the Policy Interpretation document.

- Scope: Identifies who and what the new technology affects.
- Policy Context: Identifies and concisely references relevant framework policies.
- Additional Guidance: Provides additional instructions or information on how to access more specific information.

The key advantage of the policy interpretation concept is eliminating the need for an organization to revise or produce additional top-level policies until the organization's fundamental Information Security objectives change. In practice, given the traceable development process for the Policy Framework, the change would have to be revolutionary enough to force strategic adjustments to fundamental risk management objectives.

Framework Components

As illustrated in Figure 8, the METASES Information Security Policy Framework is a hierarchical structure consisting of an Information Security Charter, seven policies, and associated standards.

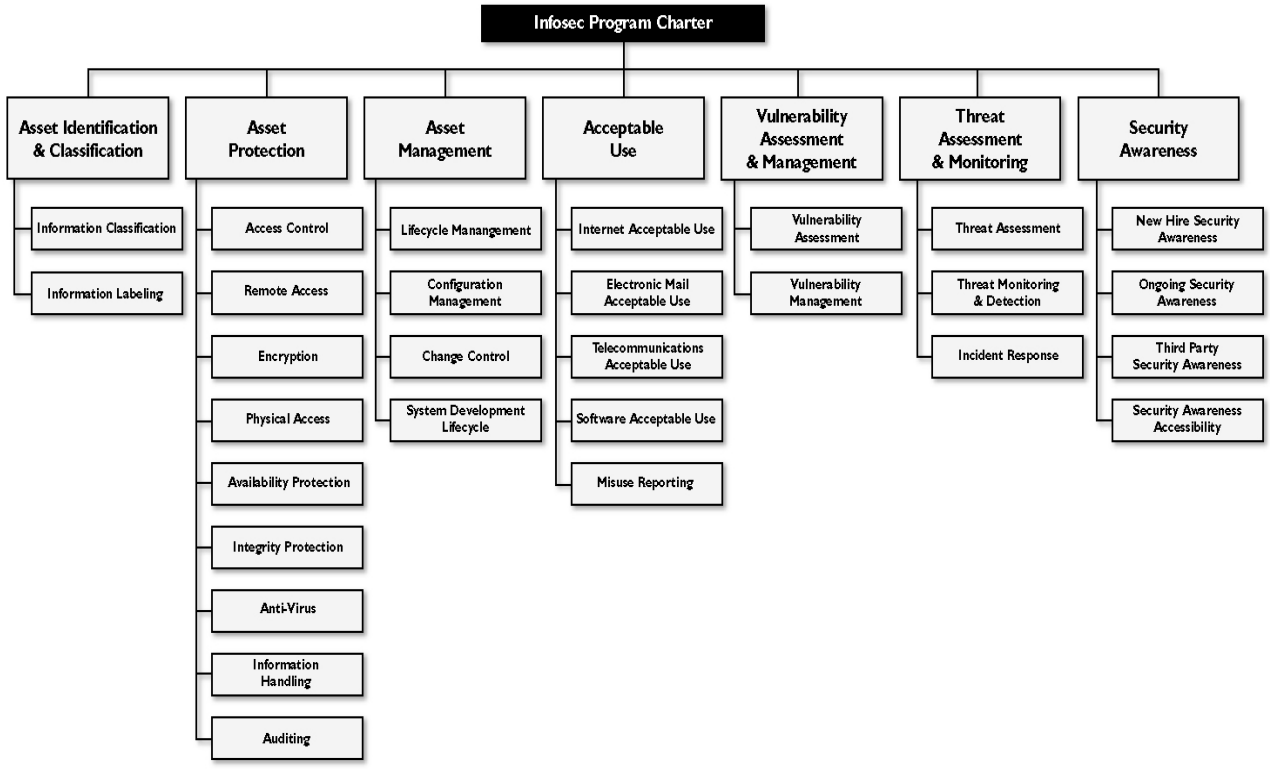

Figure 8: The META Security Group Information Security Policy Framework

Information Security Program Charter

The Information Security Program Charter serves as the capstone document for the Information Security Program and empowers the Information Security Program to manage Information Security-related business risks. The charter summarizes an organization's

attitude and philosophy regarding security, and states the mission of the Information Security Program. In addition, the charter addresses the following key program management issues:

- Scope of coverage: Identifies the assets, individuals, groups, and organizations governed by the Policy Framework.
- Executive ownership: Identifies the high-level executives with ownership responsibility for the Information Security Program.
- Management responsibility: Identifies who is responsible for managing the various aspects of the Information Security Program and maintaining the Policy Framework.
- Accountability: Identifies who is accountable for the Information Security Program and the integrity of the assets.
- Policy enforcement: Outlines the consequences for non-compliance, and methods for handling exceptions to Policy Framework elements.
- Communication: Outline how the charters, policies, and standards will be communicated.

The Chief Executive Officer should approve the Charter to provide justification and executive approval of Information Security Program activities. Without this approval, Information Security-related initiatives and activities may be challenged and require individual justification and approval.

Sample Information Security Program Charter

Information is an essential Company ABC asset and is vitally important to Company ABC's business operations and long-term viability. Company ABC must ensure that its information assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Company ABC's Information Security Program will adopt a risk management approach to Information Security. The risk management approach requires the identification, assessment, and appropriate mitigation of vulnerabilities and threats that can adversely impact Company ABC's information assets.

This *Information Security Program Charter* serves as the "capstone" document for the Company ABC Information Security Program. Policies further define the Information Security objectives in topical areas. Standards provide more measurable guidance in each policy area. Procedures describe how to implement the standards.

I. Scope

This *Information Security Program Charter* and associated policies, standards, guidelines, and procedures apply to all employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems.

II. Information Security Program Mission Statement

The Company ABC Information Security Program will use a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures that address security objectives in tandem with business and operational considerations.

The Information Security Program will protect information assets by developing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

The Information Security Program will reduce vulnerabilities by developing policies to assess, identify, prioritize, and manage vulnerabilities. The management activities will support organizational objectives for mitigating the vulnerabilities as well as developing and using metrics to gauge improvements in vulnerability mitigation.

The Information Security Program will counter threats by developing policies to assess, identify, prioritize, and monitor threats. The monitoring activities will support organizational objectives for deterring, responding to, and recovering from threats. The monitoring activities also will support the development and use of metrics to gauge the level of threat activity and the effectiveness of the Company ABC threat detection and response capabilities.

The Information Security Program will ensure that the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to educate and train the individuals, groups, and organizations covered by the scope of this Charter.

III. Ownership and Responsibilities

The Chief Executive Officer (CEO) approves the Company ABC Information Security Program Charter. The Information Security Program Charter assigns executive ownership of and accountability for the Company ABC Information Security Program to the Chief Information Officer (CIO). The CIO must approve Information Security policies.

The CIO will appoint a Chief Information Security Officer (CISO) to implement and manage the Information Security Program across the organization. The CISO is responsible for the development of Company ABC Information Security policies, standards and guidelines. The CISO must approve Information Security standards and guidelines, and ensure their consistency with approved Information Security policies. The CISO also will establish an Information Security Awareness Program to ensure that the Information Security Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood across the organization.

Company ABC management is accountable for the execution of the Company ABC Information Security Program and ensuring that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving and implementing Information Security procedures in their organizational units, and ensuring their consistency with approved Information Security policies and standards.

All individuals, groups, or organizations identified in the scope of this Charter are responsible for familiarizing themselves with the Company ABC Information Security Program Charter and complying with its associated policies.

IV. Enforcement and Exception Handling

Failure to comply with Company ABC Information Security policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to Company ABC Information Security policies, standards, and guidelines should be submitted to the approval authorities designated in the policies, standards, and guidelines. Exceptions shall be permitted only on receipt of written approval from an authorized approval authority.

V. Review and Revision

The Company ABC Information Security policies, standards, and guidelines shall be reviewed under the supervision of the CISO, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness. A formal report comprising the results and any recommendations shall be submitted to the CIO.

Approved: _____

Signature
<Typed Name>
Chief Executive Officer

Company ABC ISPC-MMDDYY-#

Policies

A policy defines an organization's high-level Information Security philosophy in a topical area. Policies are brief technology- and solution-independent documents. However, policies provide the necessary authority to establish and implement technology- and solution-specific standards. In general, policies remain relevant and applicable for a substantial period of time, and only require revisions when there is a fundamental change to an organization's business or operational objectives and environment.

META Security Group has found through its extensive experience with clients that an Information Security policy within a comprehensive and practical framework has the following characteristics:

- Both senior management and users must accept the policy as the official reference document on security. The document should be introduced with a statement from executive management (for example, the CEO or CIO) that confirms top management's commitment to the policy principles.

- The policy should firmly integrate security within the overall business and technical strategies, and within risk management practices.

- The business should drive the policy and policy enforcement, not the other way around.

- The policy must be consistent with existing corporate directives and guidelines, and with applicable government legislation and regulations.

- The scope of the policy is one of the most important characteristics. As early as possible in the process, an organization should define what resources are affected, and to whom the policy applies (for example, all employees, full-time employees only, contractors, consultants, or customers).

- The policy should be restricted in its reach and clear in its organization. It should be limited to stating the organization's security objectives, priorities, and high-level strategies, thus serving as a framework for the various business areas. It should be concise, and written in clear, unambiguous language that speaks directly to a broad audience. It should be carefully structured to allow easy reference to particular sections.

- As a living document, the policy should be reviewed at regular intervals, or as significant events, such as a merger or an acquisition, require. It should be flexible enough to deal with new and rapidly changing technology landscapes without having to be constantly rewritten. It should be modular enough to modify fairly easily without triggering a cascade of required changes.

- The policy should focus exclusively on broad principles and objectives. It is intended as a living reference document, for use over a long period. Every contingency or every implementation detail cannot be foreseen. Details on how to apply the policy to areas that are more often updated, such as individual business practices or computing resources, should be addressed in supporting documents such as standards or procedure manuals.

- The policy document must be carefully worded. It is very important to ensure that all terms are accurately and precisely defined, and used exactly as intended. Each concept should be carefully but broadly defined, not in relation to a particular technology.

- The policy should clearly delineate responsibility, accountability, and lines of authority across the organization. These provide a solid definition of what is expected of people inside and outside of the organization, and outline exactly how to accomplish these expectations.

- The policy must be technically and organizationally feasible. It must take a realistic approach to what can be accomplished with current technology, or to what is practical for procedural enforcement, within the constraints of the organization's culture and

mission. A security policy will likely have little to do with technology, or with what it alone can accomplish.

- The various constituents governed by the policy should have access to and read and understand only relevant material, rather than being required to read and understand all of the policy information. This will improve compliance with the policy. While "ignorance of the law" should not excuse its violation, practicality suggests that a more minimalist approach to policy is preferred. With this approach, personnel will actually understand what matters most in the performance of their jobs.

- Each policy should clearly describe how exceptions to the policy are considered and adjudicated.

- The initial policy document, and subsequent updates, should have a version number and a date. All policy documents should be in a centrally managed change control system that keeps a log of modifications.

The high-level objectives established in the Information Security Program Charter lead directly to the following seven policies:

1. Asset Identification and Classification
2. Asset Protection
3. Asset Management
4. Acceptable Use
5. Vulnerability Assessment and Management
6. Threat Assessment and Monitoring
7. Security Awareness

The policies are explained in the sections that follow.

Asset Identification and Classification Policy

The Asset Identification and Classification Policy defines an organization's objectives for establishing specific standards to define, identify, classify, and label information assets. An organization must properly classify the information assets relative to its criticality, sensitivity, and value to the organization. Typically, this policy identifies no more than five information classifications (for example, Restricted, Confidential, Internal Use Only, Public).

Sample Asset Identification and Classification Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of

Company ABC information assets.

This *Asset Identification and Classification Policy* defines Company ABC's objectives for establishing specific standards on the identification, classification and labeling of Company ABC's information assets.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

An information asset is defined as all data, whether in the form of electronic media, physical records, or data originated, taken or summarized from these sources, that is used by Company ABC or in support of Company ABC business processes, including all data maintained or accessed through systems owned or administered by or on the behalf of Company ABC.

II. Objectives

Company ABC defines information classifications based on the sensitivity, criticality, and value of the information. All information assets, whether generated internally or externally, must be categorized into one of these information classifications: Restricted, Confidential, Internal Use Only, or Public. When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. Specific instructions for classifying information assets are provided in the *Information Classification Standard*.

All Restricted, Confidential, and Internal Use Only information must be labeled or marked with the appropriate information classification designation. Such markings must appear on all manifestations of the information. Specific instructions for labeling information assets are provided in the *Information Labeling Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Identification and Classification Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation and maintenance of the *Asset Identification and Classification Policy* and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company ABC information assets:

- Owners are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CIO will make the designation. Owners are responsible for: identifying information assets; assigning the proper information classification; ensuring the proper labeling for sensitive information; designating the Custodian in possession of the information; ensuring the information classifications are properly communicated and understood by the Custodians; and reviewing information assets periodically to determine if their classifications should be changed.

- Custodians are the managers, administrators and those designated by the Owner to manage, process or store information assets. Custodians are responsible for understanding the information classifications, and applying the necessary controls (specified in the *Asset Protection Policy*) to

maintain and conserve the information classifications and labeling established by the Owners.

- Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for understanding the information classifications, abiding by the controls defined by the Owner and implemented by Custodians; maintaining and conserving the information classification and labeling established by the Owners; and contacting the Owner when information is unmarked or the classification is unknown.

IV. Enforcement and Exception Handling

Failure to comply with the *Asset Identification and Classification Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Identification and Classification Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Identification and Classification Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Asset Protection Policy

The Asset Protection Policy defines an organization's objectives for establishing specific standards for providing an appropriate degree of confidentiality, integrity, and availability for information assets. The Asset Protection Policy in the META Security Group Information Security Policy Framework is a "superset" of more narrowly focused policies such as Authorization and Authentication that are sometimes encountered in other policy implementations.

Sample Asset Protection Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Asset Protection Policy* defines Company ABC objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification*

Policy.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Authorization for access to information assets will be based on the classification of the information and defined to provide only the level of access required to meet an approved business need or perform prescribed job responsibilities. Proper identification and authentication are required. Specific instructions for controlling access to information assets are provided in the *Access Control Standard*.

Authorization for remote access to information assets will be provided only to meet an approved business need or perform prescribed job responsibilities. Remote access must be facilitated by using Company ABC approved methods and programs. Specific instructions for accessing information assets remotely are provided in the *Remote Access Standard*.

Information assets must be protected with physical access control of areas containing information assets or processing activities. The physical access controls must be commensurate with the classification of the information and defined to provide only the level of physical access required to meet an approved need or perform prescribed job responsibilities. Specific instructions for physical access to information assets are provided in the *Physical Access Standard*.

Encryption must be used to protect Restricted and Confidential information assets that will be transmitted over non-secure or public networks. Storage of Restricted and Confidential information assets must be achieved with similar approved encryption methods. Only Company ABC-approved encryption algorithms and products can be used to protect Restricted and Confidential information. Specific instructions for encryption are provided in the *Encryption Standard*.

Information assets must be created and maintained with appropriate controls to ensure that the information is correct, auditable, and reproducible. Specific instructions for protecting the integrity of information assets are provided in the *Integrity Protection Standard*.

Company ABC must establish appropriate controls to ensure information assets are consistently available to conduct business. Business continuity planning to effectively back up, replicate, and recover information assets, as necessary, must be established. Specific instructions for protecting the availability of information assets are provided in the *Availability Protection Standard*.

Information assets must be protected from destructive software elements such as viruses and malicious code that impair normal operations. Company ABC-approved virus detection programs must be installed, enabled, and updated on all systems susceptible to viruses and malicious code. Specific instructions for protecting information assets from viruses and malicious code are provided in the *Anti-Virus Standard.*

Auditing must be activated to record relevant security events. The audit logs must be securely maintained for a reasonable period of time. Specific instructions for auditing information assets are provided in the *Auditing Standard.*

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Protection Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Asset Protection Policy* and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company ABC information assets:

- Owners are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CIO will make the designation. Owners are responsible for defining procedures that are consistent with the *Asset Protection Policy* and associated standards, ensuring the confidentiality, integrity and availability of information assets; authorizing access to those who have an approved business need for the information; and ensuring the revocation of access for those who no longer have a business need for the information.

- Custodians are the managers, administrators, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for: providing a secure processing environment that protects the confidentiality, integrity and availability of information; administering access to information as authorized by the Owner; and implementing procedural safeguards and cost-effective controls.

- Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for using the information only for its intended purposes, and for maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Asset Protection Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Protection Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Protection Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Asset Management Policy

The Asset Management Policy defines an organization's objectives for properly managing its Information Technology infrastructure, including networks, systems, and applications that store, process and transmit information assets throughout the entire life cycle. This policy ensures that the organization's infrastructure is designed, implemented, and maintained to support the protection objectives established in the Asset Protection Policy.

Sample Asset Management Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Asset Management Policy* defines Company ABC's objectives for establishing specific standards for the management of the networks, systems, and applications that store, process and transmit Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC systems, including hardware and software, must be managed in accordance with the information asset protection objectives established in the *Asset Protection Policy* throughout the life cycle from acquisition to disposal. Specific instructions for life cycle management of Company ABC hardware and software are provided in the *Life Cycle Management Standard*.

Company ABC will establish and maintain baseline configuration standards in accordance with the information asset protection objectives established in the *Asset Protection Policy* for each system represented in the Company ABC production environment. Specific instructions for configuration management are provided in the *Configuration Management Standard*.

All systems, networks and applications used in the Company ABC production environment must follow the documented change control process and procedures to ensure that only authorized updates or changes are made. Specific instructions for change control are provided in the *Change Control Standard*.

All production systems and applications developed by Company ABC or on behalf of Company ABC must adhere to the documented process of analyzing, designing, developing, testing, and enhancing systems to ensure the integration of appropriate security controls. Specific instructions for systems development are provided in the *System Development Life Cycle Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Management Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Asset Management Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Asset Management Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the *Asset Management Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Asset Management Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Asset Management Policy* and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Management Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Management Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Company ABC AMP-MMDDYY-#

Acceptable Use Policy

The Acceptable Use Policy defines an organization's objectives for ensuring the appropriate business use of information assets. The policy covers appropriate use of an organization's information and telecommunications systems and equipment including, but not limited to, Internet, electronic mail, telephones, voice mail, pagers, and faxes. The policy also states an organization's position on the right to monitor, record, and audit the use of such systems and equipment, and addresses reporting of potential misuse.

Sample Acceptable Use Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by

establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Acceptable Use Policy* defines Company ABC objectives for establishing specific standards on appropriate business use of Company ABC's information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC information and telecommunications systems and equipment, including Internet, electronic mail, telephone, pager, voice mail and fax, are provided for official and authorized Company ABC business purposes. Any use of such systems and equipment perceived to be illegal, harassing, offensive, or in violation of other Company ABC policies, standards or guidelines, or any other uses that would reflect adversely on Company ABC, can be considered a violation of this policy.

Company ABC reserves the right to monitor, record, or periodically audit use of any of its information and telecommunications systems and equipment. Use of these systems and equipment constitutes expressed consent by those covered by the scope of this policy to such monitoring, recording, and auditing. Actual or suspected misuse of these systems should be reported to the appropriate Company ABC management representative in a timely manner. Specific instructions for reporting misuse of Company ABC information and telecommunications systems and equipment are provided in the *Misuse Reporting Standard*.

Specific instructions for appropriate business use of the Internet are provided in the *Internet Acceptable Use Standard*.

Specific instructions for appropriate business use of the Company ABC electronic mail system are provided in the *Electronic Mail Acceptable Use Standard*.

Specific instructions for appropriate business use of telephones, pagers, faxes, and voice mail are provided in the *Telecommunication Acceptable Use Standard*.

Specific instructions for appropriate business use of software and programs are provided in the *Software Acceptable Use Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Acceptable Use Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Acceptable Use Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Acceptable Use Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the *Acceptable Use Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Acceptable Use Policy* and associated standards and guidelines.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Acceptable Use Policy* and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Acceptable Use Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Acceptable Use Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Company ABC AUP-MMDDYY-#

Vulnerability Assessment and Management Policy

The Vulnerability Assessment and Management Policy defines an organization's objectives for vulnerability assessment activities and ongoing vulnerability management efforts. A vulnerability assessment is an activity in which an organization identifies and prioritizes technical, organizational, procedural, administrative, or physical security weaknesses. A vulnerability assessment should yield a traceable, prioritized "road map" for mitigating the assessed vulnerabilities. Vulnerability management is the actual process of mitigating risks, and maintaining metrics on the organization's progress in doing so.

Sample Vulnerability Assessment and Management Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will reduce vulnerabilities by establishing policies to assess, identify, prioritize, and manage vulnerabilities.

This *Vulnerability Assessment and Management Policy* defines Company ABC's objectives for establishing specific standards for the assessment and ongoing management of vulnerabilities.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

Vulnerabilities are the exploitable weaknesses in information system and procedures, including technical, organizational, procedural, administrative, or physical weaknesses.

II. Objectives

Company ABC will periodically assess and identify vulnerabilities in the Company ABC information systems environment and procedures. Specific instructions for assessing vulnerabilities are provided in the *Vulnerability Assessment Standard.*

Findings from the vulnerability assessment activities must be used to develop a formal plan for the ongoing elimination or mitigation of the vulnerabilities. Company ABC must establish associated metrics for gauging the effectiveness of these plans. Specific instructions for managing vulnerabilities are provided in the *Vulnerability Management Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Vulnerability Assessment and Management Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Vulnerability Assessment and Management Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Vulnerability Assessment and Management Policy* and associated standards, guidelines and procedures can result in disciplinary actions, up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Vulnerability Assessment and Management Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Vulnerability Assessment and Management Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature <Typed Name> Chief Information Officer Company ABC	VAMP-MMDDYY-#

Threat Assessment and Monitoring Policy

The Threat Assessment and Monitoring Policy defines an organization's objectives for threat assessment activities and ongoing threat monitoring efforts. A threat assessment is an activity in which an organization identifies and prioritizes categories of threats or specific threats sources (for example, organizations, people) that may be relevant to the defined assets, as well as typical vulnerabilities present within the organization. The organization then should seek to deter such threats (for example, through warning banners, legal notices, etc.)

The organization also should implement threat monitoring to detect, respond to, and support recovery from threat activity. This monitoring typically will include automated activities (for example, intrusion detection system installation and operation) and manual procedures (for example, log reviews).

Sample Threat Assessment and Monitoring Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will counter threats by establishing policies to assess, identify, prioritize, and monitor threats.

This *Threat Assessment and Monitoring Policy* defines Company ABC's objectives for establishing specific standards for the assessment and ongoing monitoring of threats to Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

Threats are the intentional or accidental actions, activities or events that can adversely impact Company ABC information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.

II. Objectives

Company ABC will periodically identify, analyze, and prioritize threats to information assets. Finding from the threat assessment activities will be integrated, as appropriate, into the Security Awareness Program. Specific instructions for assessing threats are provided in the *Threat Assessment Standard.*

Company ABC will perform real-time intrusion detection monitoring and periodic intrusion detection

analysis to detect threat and intrusion activity. Company ABC must establish and track representative metrics for gauging progress in this area. Specific instructions for monitoring and detecting threats are provided in the *Threat Monitoring and Detection Standard*.

Company ABC will develop and exercise formal plans for responding to Information Security intrusions and incidents. Company ABC must establish associated metrics for gauging the effectiveness of these plans. Specific instructions for responding to Information Security incidents are provided in the *Incident Response Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Threat Assessment and Monitoring Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Threat Assessment and Monitoring Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving, and implementing procedures in its organizational units, and ensuring their consistency with the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Threat Assessment and Monitoring Policy* and associated standards, guidelines, and procedures can result in disciplinary actions, up to and including termination of employment for employees, or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Threat Assessment and Monitoring Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Threat Assessment and Monitoring Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Security Awareness Policy

The Security Awareness Policy defines an organization's objectives for establishing a formal Security Awareness Program. This policy ensures that the Policy Framework elements are properly communicated and accessible to new hires, employees, and third parties such as contractors, partners, and consultants. This policy also ensures that appropriate education and training are provided.

Sample Security Awareness Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will ensure that the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to facilitate awareness.

This *Security Awareness Policy* defines Company ABC objectives for establishing a formal Security Awareness Program, and specific standards for the education and communication of the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC's Information Security Program Charter and relevant policies, standards, and guidelines must be properly communicated to and understood by all newly hired Company ABC employees. Newly hired Company ABC employees must be provided with the appropriate security awareness education and training. Specific instructions for providing security awareness education and training for new Company ABC employees are provided in the *New Hire Security Awareness Standard*.

Company ABC's Information Security Program Charter and relevant policies, standards, and guidelines must be properly communicated to and understood by all contractors, partners and consultants. Specific instructions for providing security awareness education and training for contractors, partners, and consultants are provided in the *Third Party Security Awareness Standard*.

All Company ABC employees will be provided with recurring and ongoing education and training to ensure continue awareness, and address emerging risks or topics of interest. Specific instructions for providing security awareness education and training for Company ABC employees are provided in the *Ongoing Security Awareness Standard*.

All Company ABC employees will be provided appropriate access to the *Information Security Program Charter* and relevant policies, standards, and guidelines. Specific instructions are provided in the *Security Awareness Accessibility Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Security Awareness Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Security Awareness Policy* and the associated standards and guidelines.

Company ABC management is responsible for ensuring that the *Security Awareness Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units.

All individuals, groups or organizations identified in the scope of this policy are responsible for familiarizing themselves with and complying with the *Security Awareness Policy* and associated standards, guidelines, and procedures.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Security Awareness Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees, or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Security Awareness Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Security Awareness Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Company ABC SAP-MMDDYY-#

Standards

The seven policies described in the previous section provide full topical coverage for an Information Security Program established to support the risk management objectives established in the Charter. In contrast, specific key standards provide more measurable criteria for satisfying and supporting the high-level objectives defined and authorized by the policies themselves. As opposed to policies, standards may be technology or solution-specific.

The following section outlines the standards that support the policies described above.

Asset Identification and Classification Standards

The following key standards support the Asset Identification and Classification Policy:

- Information Classification
- Information Labeling

The Information Classification Standard provides the definitions for the information classification scheme established in the Asset Identification and Classification Policy. More specifically, these definitions outline the attributes and criteria for each of the information classifications, and provide relevant examples. In addition, the standard provides guidance on how to classify information assets and addresses default classification, reclassification, and declassification.

The Information Labeling Standard clearly states how an information asset must be labeled or marked based on its classification. Labels may be placed on printed material (for example, as cover sheets or header/footer text), on physical systems, or on files and database elements, depending on the specifics of the standard.

Asset Protection Standards

The following key standards support the Asset Protection Policy:

- Access Control
- Remote Access
- Encryption
- Physical Access
- Integrity Protection
- Availability Protection
- Anti-virus
- Information Handling
- Auditing

In other policy frameworks and implementations, these standards usually exist as "policies." Such an approach violates the basic definition of policy by focusing on specific systems and technologies that will change often.

The Assess Control Standard states how information assets are protected, who is authorized access, and under what conditions. The standard establishes identification and authentication requirements including, but not limited to, unique identifiers, passwords, and formats. In addition, the standard addresses approval and deactivation requirements.

The Remote Access Standard states how and under what conditions information assets are accessed remotely. The standard identifies an organization's approved remote access technologies and methods including modems, VPNs, extended authentication, as well as modes and points of entry.

The Encryption Standard states how sensitive information assets are encrypted in transmission and storage. The standard identifies an organization's approved encryption technologies and methods, including algorithms, key selection, and software and hardware.

The Physical Access Standard states how the information assets will be physically protected. The standard establishes requirements including, but not limited to, building access, server room access, and work area or clean desk safeguards.

The Integrity Protection Standard states how the integrity of information assets will be maintained. The standard establishes integrity requirements including separation of duties, rotation of assignments, as well as organization-approved technologies that utilize checksum and hashing algorithms.

The Availability Protection Standard states how the availability of information assets will be protected. The standard establishes availability requirements, including the frequency of backups and replication, as well as recovery criteria.

The Anti-Virus Standard states how information assets will be protected from virus and malicious code. The standard establishes an organization's approved methods and technologies, update frequency for virus signatures, and prevention guidance.

The Information Handling Standard states how information assets will be handled based on their information classification. The standard establishes an organization's approved methods of handling printed information, as well as electronically stored and transmitted information.

The Auditing Standard establishes auditing or logging requirements, including activation, retention period, protection, and storage.

Asset Management Standards

The following key standards support the Asset Management Policy:

- Life Cycle Management
- Configuration Management
- Change Control
- System Development Life Cycle

The Life Cycle Management Standard establishes the requirements for ensuring that networks, systems and applications are appropriately managed throughout the typical life cycle process, including development, implementation, and end-of-life. The end-of-life aspect of the life cycle process is especially important to ensure an organization clearly understands what to do from a security perspective with information or systems that are no longer needed to support business operations.

The Configuration Management Standard establishes the requirements for maintaining baseline configuration standards for systems used in the production environment. The baseline configuration standards formally documents and defines specific configuration requirements that are consistent with the protection objectives in the Asset Protection Policy.

The Change Control Standard establishes the requirements for following approved processes and procedures that ensure only authorized updates and changes are implemented in the production environment.

The Systems Development Life Cycle Standards establishes the requirements for ensuring that security controls are built into systems and applications that are developed in-house or by third parties.

In addition, since many organizations do not have a formal tracking system, hardware and software inventory requirements are usually represented in the form of a guideline or "standard in waiting."

Acceptable Use Standards

The following key standards support the Acceptable Use Policy:

- Internet Acceptable Use
- Electronic Mail Acceptable Use
- Telecommunications Acceptable Use
- Software Acceptable Use
- Misuse Reporting

The Internet Acceptable Use Standard states how an organization's Internet resources should be appropriately used in conjunction with valid work or project-related requirements.

The Electronic Mail Acceptable Use Standard states how an organization's electronic mail resources should be appropriately used in conjunction with valid work or project-related requirements.

The Telecommunications Acceptable Use Standard states how an organization's telecommunications resources should be appropriately used in conjunction with valid work or project-related requirements.

The Software Acceptable Use Standard provides "auditable" instruction on compliance with licensing agreements and download restrictions.

The Misuse Reporting Standard states the responsibility for reporting suspected misuse of information assets. The standard further defines misuse, identifies to whom suspected misuse will be reported, and outlines escalation approaches.

Vulnerability Assessment and Management Standards

The following key standards support the Vulnerability Assessment and Management Policy:

- Vulnerability Assessment
- Vulnerability Management

The Vulnerability Assessment Standard establishes the requirement for ongoing review (for example, by the Information Security team) of vulnerability information, as well as periodic formal vulnerability assessments of defined scope. In addition, the standard describes how to prioritize vulnerabilities.

The Vulnerability Management Standard establishes the requirements for developing and executing a plan to address discovered vulnerabilities. In addition, the standard establishes representative metrics for tracking progress.

Threat Assessment and Monitoring Standards

The following key standards support the Threat Assessment and Monitoring Policy:

- Threat Assessment
- Threat Monitoring and Detection
- Incident Response

The Threat Assessment Standard establishes the requirement for periodic identification, analysis, and prioritization of threats to the organization's Information Security objectives.

The Threat Monitoring Standard provides "auditable" instruction and guidance for performing real-time monitoring as well as periodic, more in-depth monitoring and analysis to detect threat and intrusion activity. In addition, this standard establishes representative metrics for tracking progress in this area.

The Incident Response Standard establishes the requirements for responding to detected threat and intrusion activity. In addition, this standard addresses incident response plan development and execution, as well as the associated metrics.

Security Awareness Standards

The following key standards support the Security Awareness Policy:

- New Hire Security Awareness

- Third Party Security Awareness
- Ongoing Security Awareness
- Security Awareness Accessibility

The New Hire Security Awareness Standard establishes the requirements for educating and training new employees on the Information Security Program Charter and relevant policies.

The Third Party Security Awareness Standard establishes the requirements for educating and training contractors, partners and consultants on the Information Security Program Charter and relevant policy documentation.

The Ongoing Security Awareness Standard establishes the requirements for providing ongoing education and training to employees on emerging risks and topics of interest.

The Security Awareness Accessibility Standard established the requirements for providing appropriate access to the Information Security Program Charter and relevant policies, standards and guidelines (refer to Appendix C).

Practical Use of the Framework

The METASES Information Security Policy Framework was developed to provide a practical baseline reference model that an organization could use and customize to address its specific needs and requirements. Figure 9 illustrates the high-level process used by META Security Group in its policy assessment and gap analysis consulting engagements.

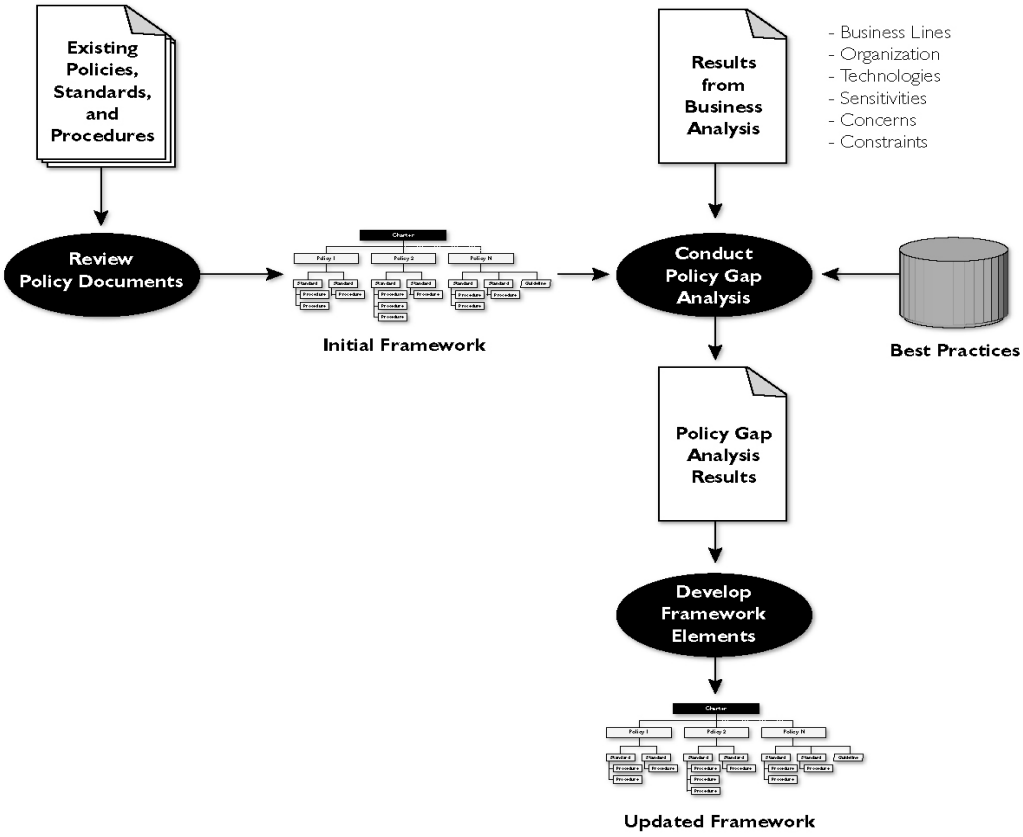

Figure 9: High-Level, practical use of the Framework

META Security Group anticipates that an organization can use the Policy Framework in a similar manner. More specifically, organizations will use the Policy Framework to:

- Review and assess their current security policies.
- Conduct policy gap analysis.
- Develop and revise Information Security policies and standards.

Policy Review

The META Security Group Information Security Policy Framework serves a best practices reference for reviewing or assessing an organization's current Information Security policies, standards, guidelines and procedures. Many organizations already have a significant amount of Information Security policy documentation. Using the Framework as a reference, an organization should review and analyze its existing policy documentation to develop an Initial Policy Framework that translates its currently intertwined policies, standards, guidelines and procedures into a comprehensive hierarchical framework. This translation process involves reviewing topical coverage, determining placement of existing policy documents in the framework hierarchy and creating a nominal mapping. This translation is important in that it will allow an organization to inventory and clearly identify the relationships between current policy elements.

Policy Gap Analysis

Having established an Initial Policy Framework that nominally maps existing policy documents into a hierarchical framework, organizations should conduct a Policy Gap Analysis. In addition to the Initial Policy Framework, the Policy Gap Analysis must leverage the results of a formal business analysis or other sources that document the organizational structure, various lines of business, and technologies, as well as sensitivities, concerns, and constraints. The Policy Gap Analysis will identify missing Policy Framework elements as well as elements that are ineffectual or unenforceable. Missing elements are those that should be present but are not included in the Initial Policy Framework. Ineffectual elements are those that are present but are either unclear, lacking impact, or missing key components. Unenforceable elements include those that have proven unenforceable in the organization's current implementation.

Policy Development

Organizations should use the results of the Policy Gap Analysis to set priorities for refining and developing Policy Framework elements. The sample policies in this document are provided to illustrate how the policy objectives are traceable back to the risk management and business objectives contained in the Charter. Moreover, these sample policies can be customized and used in policy revision and development efforts. However, organizations should revise, develop and coordinate the Policy Framework elements in a "top down" manner. This approach will allow organizations to reach agreement with key stakeholders on the policies, before pursuing development of the underlying standards and procedures.

Practical Issues

The META Security Group Information Security Policy Framework was designed to be comprehensive and practical. The Framework provides a baseline reference model that organizations can customize to address their specific needs based on business requirements, culture, industry regulations, and other considerations. META Security Group has identified the following issues that an organization may need to address when using this Framework as a reference:

- Some organizations must adhere to regulatory requirements that are not explicitly referenced or adequately addressed in this discussion of the Policy Framework. These regulatory requirements should be specifically identified and incorporated into the Information Security Program Charter and associated policies, standards, and guidelines. For example, policy enforcement and exception handling would need to specifically reference regulations that would result in legal or disciplinary actions.

- Some organizations will need to customize the Framework to reflect and address industry-specific audit requirements. This may involve a specific change to the policy structure or content to pass the audit or ease the audit process. For example, banking organizations may want their policy framework to align with the items covered in the Federal Deposit Insurance Corporation Safety and Soundness Examination for electronic banking. This may include semantics such as referring to "Incident Response" as "Incident Response and Preparedness".

- Some of the definitions discussed in this Policy Framework may contradict or inadequately address an organization's requirements. For example, an organization may require a broader or more specific definition of information or information assets. On the surface, this may appear to be a trivial change or replacement in the Asset Identification and Classification Policy. However, this definition supports other framework elements such as Asset Protection and Asset Management. An organization needs to ensure that the related framework elements are consistent with the new definition.

- The organizational structure of a company may dictate changes to some of the responsibility assignments in the Framework. For example, the responsibilities of the CIO may be assigned to the CISO in some organizations. In a decentralized organization, the CISO responsibilities may be delegated to security officers or directors of individual business units. In addition, the term "Company ABC management" referred to in the sample policies may be changed to reflect the organizational structure and identify the specific managers (for example, division managers, vice presidents, and business unit heads).

- Some organizations will need to customize the roles of responsibility for Owner, Custodian, and User discussed in this Framework to adequately address their specific requirements. In many organizations, the IT department handles the responsibility of designating custodians.

- The sample policies in this document have simply referenced the exception handling procedure and process. However, an organization will actually need to develop specific procedures for requesting an exception, including identifying the policy topic or objective, business case, risks involved, and desired duration. In addition, a formal process involving appropriate levels of management must be established to accept or reject the exception requests.

- Some organizations are currently using or will require a different information classification scheme. The information classification scheme referenced in this Policy Framework consists of four classifications: Restricted, Confidential, Internal Use Only, and Public. Information that is also proprietary would be considered an "instance" of the Restricted, Confidential, and Internal Use Only classifications instead of an additional classification. For example, a proposal would be labeled or marked as "Company ABC Confidential and Proprietary" since it contains confidential data such as pricing, as well as proprietary data such as project approaches and methodologies.

- Some organizations have documented technical standards and procedures for hardening or configuring operating systems and applications. For example, an organization may have a Windows NT server standard. This type of technical standard supports the objectives outlined in both the Asset Management and Asset Protection policies. The Asset Management Policy establishes the organization's configuration management objectives for setting up and maintaining approved configurations. In addition, an organization would need to ensure that the approved configurations, such as a Windows NT server standard, address all of the relevant Asset Protection standards, including Access Control, Remote Access, Encryption, and Auditing.

- Many organizations use a policy cover page to identify the policy and capture updates or versions. At a minimum, the cover page should including the policy name, date, version number, and company name. In addition, this information should be captured in the header or footer of the document.

Conclusion

METASES recognizes that the Information Security Policy Framework, including the establishment of the Charter, seven policies, and associated standards, represents a substantial departure from the current policy frameworks and implementations that organizations have used to define Information Security policy. However, the METASES Information Security Policy Framework provides a baseline reference model that is traceable to risk management and business objectives; clarifies definitions of framework elements; and provides an organization with a clear measure of completeness at the policy and standard level.

Appendix A -- Sample Charter and Policies

Sample Information Security Program Charter

Information is an essential Company ABC asset and is vitally important to Company ABC's business operations and long-term viability. Company ABC must ensure that its information assets are protected in a manner that is cost-effective and that reduces the risk of unauthorized information disclosure, modification, or destruction, whether accidental or intentional.

Company ABC's Information Security Program will adopt a risk management approach to Information Security. The risk management approach requires the identification, assessment, and appropriate mitigation of vulnerabilities and threats that can adversely impact Company ABC's information assets.

This *Information Security Program Charter* serves as the "capstone" document for the Company ABC Information Security Program. Policies further define the Information Security objectives in topical areas. Standards provide more measurable guidance in each policy area. Procedures describe how to implement the standards.

I. Scope

This *Information Security Program Charter* and associated policies, standards, guidelines, and procedures apply to all employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems.

II. Information Security Program Mission Statement

The Company ABC Information Security Program will use a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures that address security objectives in tandem with business and operational considerations.

The Information Security Program will protect information assets by developing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

The Information Security Program will reduce vulnerabilities by developing policies to assess, identify, prioritize, and manage vulnerabilities. The management activities will support organizational objectives for mitigating the vulnerabilities as well as developing and using metrics to gauge improvements in vulnerability mitigation.

The Information Security Program will counter threats by developing policies to assess, identify, prioritize, and monitor threats. The monitoring activities will support organizational objectives for deterring, responding to, and recovering from threats. The monitoring activities also will support the development and use of metrics to gauge the level of threat activity and the effectiveness of the Company ABC threat detection and response capabilities.

The Information Security Program will ensure that the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to educate and train the individuals, groups, and organizations covered by the scope of this Charter.

III. Ownership and Responsibilities

The Chief Executive Officer (CEO) approves the Company ABC Information Security Program Charter. The Information Security Program Charter assigns executive ownership of and accountability for the Company ABC Information Security Program to the Chief Information Officer (CIO). The CIO must approve Information Security policies.

The CIO will appoint a Chief Information Security Officer (CISO) to implement and manage the Information Security Program across the organization. The CISO is responsible for the development of Company ABC Information Security policies, standards and guidelines. The CISO must approve Information Security standards and guidelines, and ensure their consistency with approved Information Security policies. The CISO also will establish an Information Security Awareness Program to ensure that the Information Security Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood across the organization.

Company ABC management is accountable for the execution of the Company ABC Information Security Program and ensuring that the Information Security Program Charter and associated policies, standards, guidelines, and procedures are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving and implementing Information Security procedures in their organizational units, and ensuring their consistency with approved Information Security policies and standards.

All individuals, groups, or organizations identified in the scope of this Charter are responsible for familiarizing themselves with the Company ABC Information Security Program Charter and complying with its associated policies.

IV. Enforcement and Exception Handling

Failure to comply with Company ABC Information Security policies, standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants,

and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to Company ABC Information Security policies, standards, and guidelines should be submitted to the approval authorities designated in the policies, standards, and guidelines. Exceptions shall be permitted only on receipt of written approval from an authorized approval authority.

V. Review and Revision

The Company ABC Information Security policies, standards, and guidelines shall be reviewed under the supervision of the CISO, at least annually or upon significant changes to the operating or business environment, to assess their adequacy and appropriateness. A formal report comprising the results and any recommendations shall be submitted to the CIO.

Approved: _____

Signature
<Typed Name>
Chief Executive Officer

Sample Asset Identification and Classification Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Asset Identification and Classification Policy* defines Company ABC's objectives for establishing specific standards on the identification, classification and labeling of Company ABC's information assets.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

An information asset is defined as all data, whether in the form of electronic media, physical records, or data originated, taken or summarized from these sources, that is used by Company ABC or in support of Company ABC business processes, including all data maintained or accessed through systems owned or administered by or on the behalf of Company ABC.

II. Objectives

Company ABC defines information classifications based on the sensitivity, criticality, and value of the information. All information assets, whether generated internally or externally, must be categorized into one of these information classifications: Restricted, Confidential, Internal Use Only, or Public. When information of various classifications is combined, the resulting collection of information or new information must be classified at the most restrictive level among the sources. Specific instructions for classifying information assets are provided in the *Information Classification Standard*.

All Restricted, Confidential, and Internal Use Only information must be labeled or marked with the appropriate information classification designation. Such markings must appear on all manifestations of the information. Specific instructions for labeling information assets are provided in the *Information Labeling Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Identification and Classification Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation and maintenance of the *Asset Identification and Classification Policy* and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company ABC information assets:

- Owners are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CIO will make the designation. Owners are responsible for: identifying information assets; assigning the proper information classification; ensuring the proper labeling for sensitive information; designating the Custodian in possession of the information; ensuring the information classifications are properly communicated and understood by the Custodians; and reviewing information assets periodically to determine if their classifications should be changed.

- Custodians are the managers, administrators and those designated by the Owner to manage, process or store information assets. Custodians are responsible for understanding the information classifications, and applying the necessary controls (specified in the *Asset Protection Policy*) to maintain and conserve the information classifications and labeling established by the Owners.

- Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for understanding the information classifications, abiding by the controls defined by the Owner and implemented by Custodians; maintaining and conserving the information classification and labeling established by the Owners; and contacting the Owner when information is unmarked or the classification is unknown.

IV. Enforcement and Exception Handling

Failure to comply with the *Asset Identification and Classification Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Identification and Classification Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Identification and Classification Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Asset Protection Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Asset Protection Policy* defines Company ABC objectives for establishing specific standards on the protection of the confidentiality, integrity, and availability of Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Authorization for access to information assets will be based on the classification of the information and defined to provide only the level of access required to meet an approved business need or perform prescribed job responsibilities. Proper identification and authentication are required. Specific instructions for controlling access to information assets are provided in the *Access Control Standard*.

Authorization for remote access to information assets will be provided only to meet an approved business need or perform prescribed job responsibilities. Remote access must be facilitated by using Company ABC approved methods and programs. Specific instructions for accessing information assets remotely are provided in the *Remote Access Standard*.

Information assets must be protected with physical access control of areas containing information assets or processing activities. The physical access controls must be commensurate with the classification of the information and defined to provide only the level of physical access required to meet an approved need or perform prescribed job responsibilities. Specific instructions for physical access to information assets are provided in the *Physical Access Standard*.

Encryption must be used to protect Restricted and Confidential information assets that will be transmitted over non-secure or public networks. Storage of Restricted and Confidential information assets must be achieved with similar approved encryption methods. Only Company ABC-approved encryption algorithms and products can be used to protect

Restricted and Confidential information. Specific instructions for encryption are provided in the *Encryption Standard*.

Information assets must be created and maintained with appropriate controls to ensure that the information is correct, auditable, and reproducible. Specific instructions for protecting the integrity of information assets are provided in the *Integrity Protection Standard*.

Company ABC must establish appropriate controls to ensure information assets are consistently available to conduct business. Business continuity planning to effectively back up, replicate, and recover information assets, as necessary, must be established. Specific instructions for protecting the availability of information assets are provided in the *Availability Protection Standard*.

Information assets must be protected from destructive software elements such as viruses and malicious code that impair normal operations. Company ABC-approved virus detection programs must be installed, enabled, and updated on all systems susceptible to viruses and malicious code. Specific instructions for protecting information assets from viruses and malicious code are provided in the *Anti-Virus Standard.*

Auditing must be activated to record relevant security events. The audit logs must be securely maintained for a reasonable period of time. Specific instructions for auditing information assets are provided in the *Auditing Standard.*

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Protection Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Asset Protection Policy* and associated standards and guidelines.

The individuals, groups, or organizations identified in the scope of this policy are accountable for one or more of the following levels of responsibility when using Company ABC information assets:

- Owners are managers of organizational units that have primary responsibility for information assets associated with their functional authority. When Owners are not clearly implied by organizational design, the CIO will make the designation. Owners are responsible for defining procedures that are consistent with the *Asset Protection Policy* and associated standards, ensuring the confidentiality, integrity and availability of information assets; authorizing access to those who have an approved business need for the information; and ensuring the revocation of access for those who no longer have a business need for the information.

- Custodians are the managers, administrators, and those designated by the Owner to manage, process, or store information assets. Custodians are responsible for: providing a secure processing environment that protects the confidentiality, integrity and availability of information; administering access to information as authorized by the Owner; and implementing procedural safeguards and cost-effective controls.

- Users are the individuals, groups, or organizations authorized by the Owner to access to information assets. Users are responsible for using the information only for its intended purposes, and for maintaining the confidentiality, integrity and availability of information accessed consistent with the Owner's approved safeguards while under the User's control.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Asset Protection Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Protection Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Protection Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Asset Management Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Asset Management Policy* defines Company ABC's objectives for establishing specific standards for the management of the networks, systems, and applications that store, process and transmit Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC systems, including hardware and software, must be managed in accordance with the information asset protection objectives established in the *Asset Protection Policy* throughout the life cycle from acquisition to disposal. Specific instructions for life cycle management of Company ABC hardware and software are provided in the *Life Cycle Management Standard*.

Company ABC will establish and maintain baseline configuration standards in accordance with the information asset protection objectives established in the *Asset Protection Policy* for each system represented in the Company ABC production environment. Specific instructions for configuration management are provided in the *Configuration Management Standard*.

All systems, networks and applications used in the Company ABC production environment must follow the documented change control process and procedures to ensure that only authorized updates or changes are made. Specific instructions for change control are provided in the *Change Control Standard*.

All production systems and applications developed by Company ABC or on behalf of Company ABC must adhere to the documented process of analyzing, designing, developing, testing, and enhancing systems to ensure the integration of appropriate security controls. Specific instructions for systems development are provided in the *System Development Life Cycle Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Asset Management Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Asset Management Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Asset Management Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving and implementing procedures in its organizational units and ensuring their consistency with the *Asset Management Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Asset Management Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Asset Management Policy* and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Asset Management Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Asset Management Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Acceptable Use Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will protect information assets by establishing policies to identify, classify, define protection and management objectives, and define acceptable use of Company ABC information assets.

This *Acceptable Use Policy* defines Company ABC objectives for establishing specific standards on appropriate business use of Company ABC's information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC information and telecommunications systems and equipment, including Internet, electronic mail, telephone, pager, voice mail and fax, are provided for official and authorized Company ABC business purposes. Any use of such systems and equipment perceived to be illegal, harassing, offensive, or in violation of other Company ABC policies, standards or guidelines, or any other uses that would reflect adversely on Company ABC, can be considered a violation of this policy.

Company ABC reserves the right to monitor, record, or periodically audit use of any of its information and telecommunications systems and equipment. Use of these systems and equipment constitutes expressed consent by those covered by the scope of this policy to such monitoring, recording, and auditing. Actual or suspected misuse of these systems should be reported to the appropriate Company ABC management representative in a timely manner. Specific instructions for reporting misuse of Company ABC information and telecommunications systems and equipment are provided in the *Misuse Reporting Standard*.

Specific instructions for appropriate business use of the Internet are provided in the *Internet Acceptable Use Standard*.

Specific instructions for appropriate business use of the Company ABC electronic mail system are provided in the *Electronic Mail Acceptable Use Standard*.

Specific instructions for appropriate business use of telephones, pagers, faxes, and voice mail are provided in the *Telecommunication Acceptable Use Standard*.

Specific instructions for appropriate business use of software and programs are provided in the *Software Acceptable Use Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Acceptable Use Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Acceptable Use Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Acceptable Use Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the *Acceptable Use Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Acceptable Use Policy* and associated standards and guidelines.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Acceptable Use Policy* and associated standards, guidelines, and procedures can result in disciplinary actions up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Acceptable Use Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Acceptable Use Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Vulnerability Assessment and Management Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will reduce vulnerabilities by establishing policies to assess, identify, prioritize, and manage vulnerabilities.

This *Vulnerability Assessment and Management Policy* defines Company ABC's objectives for establishing specific standards for the assessment and ongoing management of vulnerabilities.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

Vulnerabilities are the exploitable weaknesses in information system and procedures, including technical, organizational, procedural, administrative, or physical weaknesses.

II. Objectives

Company ABC will periodically assess and identify vulnerabilities in the Company ABC information systems environment and procedures. Specific instructions for assessing vulnerabilities are provided in the *Vulnerability Assessment Standard.*

Findings from the vulnerability assessment activities must be used to develop a formal plan for the ongoing elimination or mitigation of the vulnerabilities. Company ABC must establish associated metrics for gauging the effectiveness of these plans. Specific instructions for managing vulnerabilities are provided in the *Vulnerability Management Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Vulnerability Assessment and Management Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Vulnerability Assessment and Management Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is

also responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Vulnerability Assessment and Management Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Vulnerability Assessment and Management Policy* and associated standards, guidelines and procedures can result in disciplinary actions, up to and including termination of employment for employees or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Vulnerability Assessment and Management Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Vulnerability Assessment and Management Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Threat Assessment and Monitoring Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will counter threats by establishing policies to assess, identify, prioritize, and monitor threats.

This *Threat Assessment and Monitoring Policy* defines Company ABC's objectives for establishing specific standards for the assessment and ongoing monitoring of threats to Company ABC information assets. Company ABC information assets are defined in the scope of the *Asset Identification and Classification Policy*.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

Threats are the intentional or accidental actions, activities or events that can adversely impact Company ABC information assets, as well as the sources, such as the individuals, groups, or organizations, of these events and activities.

II. Objectives

Company ABC will periodically identify, analyze, and prioritize threats to information assets. Finding from the threat assessment activities will be integrated, as appropriate, into the Security Awareness Program. Specific instructions for assessing threats are provided in the *Threat Assessment Standard.*

Company ABC will perform real-time intrusion detection monitoring and periodic intrusion detection analysis to detect threat and intrusion activity. Company ABC must establish and track representative metrics for gauging progress in this area. Specific instructions for monitoring and detecting threats are provided in the *Threat Monitoring and Detection Standard*.

Company ABC will develop and exercise formal plans for responding to Information Security intrusions and incidents. Company ABC must establish associated metrics for gauging the effectiveness of these plans. Specific instructions for responding to Information Security incidents are provided in the *Incident Response Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Threat Assessment and Monitoring Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

Company ABC management is accountable for ensuring that the *Threat Assessment and Monitoring Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units. Company ABC management is also responsible for defining, approving, and implementing procedures in its organizational units, and ensuring their consistency with the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

All individuals, groups, or organizations identified in the scope of this policy are responsible for familiarizing themselves and complying with the *Threat Assessment and Monitoring Policy* and associated standards and guidelines.

IV. Enforcement and Exception Handling

Failure to comply with the *Threat Assessment and Monitoring Policy* and associated standards, guidelines, and procedures can result in disciplinary actions, up to and including termination of employment for employees, or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Threat Assessment and Monitoring Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Threat Assessment and Monitoring Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Sample Security Awareness Policy

As stated in the Company ABC *Information Security Program Charter*, Company ABC will follow a risk management approach to develop and implement Information Security policies, standards, guidelines, and procedures. The Information Security Program will ensure that the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures are properly communicated and understood by establishing a Security Awareness Program to facilitate awareness.

This *Security Awareness Policy* defines Company ABC objectives for establishing a formal Security Awareness Program, and specific standards for the education and communication of the *Information Security Program Charter* and associated policies, standards, guidelines, and procedures.

I. Scope

All employees, contractors, part-time and temporary workers, and those employed by others to perform work on Company ABC premises, or who have been granted access to Company ABC information or systems, are covered by this policy and must comply with associated standards and guidelines.

II. Objectives

Company ABC's Information Security Program Charter and relevant policies, standards, and guidelines must be properly communicated to and understood by all newly hired Company ABC employees. Newly hired Company ABC employees must be provided with the appropriate security awareness education and training. Specific instructions for providing security awareness education and training for new Company ABC employees are provided in the *New Hire Security Awareness Standard*.

Company ABC's Information Security Program Charter and relevant policies, standards, and guidelines must be properly communicated to and understood by all contractors, partners and consultants. Specific instructions for providing security awareness education and training for contractors, partners, and consultants are provided in the *Third Party Security Awareness Standard*.

All Company ABC employees will be provided with recurring and ongoing education and training to ensure continue awareness, and address emerging risks or topics of interest. Specific instructions for providing security awareness education and training for Company ABC employees are provided in the *Ongoing Security Awareness Standard*.

All Company ABC employees will be provided appropriate access to the *Information Security Program Charter* and relevant policies, standards, and guidelines. Specific instructions are provided in the *Security Awareness Accessibility Standard*.

III. Responsibilities

The Chief Information Officer (CIO) is the approval authority for the *Security Awareness Policy*.

The Chief Information Security Officer (CISO) is responsible for the development, implementation, and maintenance of the *Security Awareness Policy* and the associated standards and guidelines.

Company ABC management is responsible for ensuring that the *Security Awareness Policy* and associated standards and guidelines are properly communicated and understood within their respective organizational units.

All individuals, groups or organizations identified in the scope of this policy are responsible for familiarizing themselves with and complying with the *Security Awareness Policy* and associated standards, guidelines, and procedures.

IV. Policy Enforcement and Exception Handling

Failure to comply with the *Security Awareness Policy* and associated standards, guidelines and procedures can result in disciplinary actions up to and including termination of employment for employees, or termination of contracts for contractors, partners, consultants, and other entities. Legal actions also may be taken for violations of applicable regulations and laws.

Requests for exceptions to the *Security Awareness Policy* should be submitted to <Title>. Exceptions shall be permitted only on receipt of written approval from <Title>.

V. Review and Revision

The *Security Awareness Policy* will be reviewed and revised in accordance with the *Information Security Program Charter*.

Approved: _____

Signature
<Typed Name>
Chief Information Officer

Appendix B – Sample Policy Interpretation

Introduction

Company ABC acknowledges that wireless technologies are currently not suitable for use as a full-service, heavy-duty network access device. Moreover, as an evolving technology, there are several risks to consider including unauthorized access, introduction of vulnerabilities, as well as physical risk factors such as loss and theft. Nevertheless, Company ABC Wireless recognizes that wireless technologies are viable alternatives for providing periodic network access to Internal Use Only and Public Company ABC information.

This Wireless Policy Interpretation document provides guidance as it relates to existing Company ABC Information Security policies and a definitive context for the use of wireless hand-held devices to transmit, store, or originate Company ABC information assets.

Scope

This document applies to all those authorized to access Company ABC information or systems using wireless hand-held devices including Palm Pilots, WAP phones, and devices running Windows CE.

Policy Context

Asset Identification and Classification:

- Only information that has been classified and labeled as Internal Use Only or Public can be transmitted, stored or originated on wireless hand-held devices.

- Currently, these devices lack the support for strong authentication, Company ABC-approved encryption algorithms, physical risk factors, and auditing. Hence, the transmission, storage or origination of Company ABC Restricted and Confidential information on these devices is not allowed. Company ABC will continue to evaluate these devices for improvements.

Asset Protection:

- The Company ABC Internal Use Only and Public information transmitted, stored or originated on the wireless hand-held devices must be protected in accordance with the Asset Protection Policy and associated standards and guidelines.

- The password features of the wireless hand-held devices must be used although they are relatively easy to circumvent.

- Only Company ABC-approved programs can be installed (refer to list of company ABC-approved programs).

- Encryption, by means of a Company ABC-approved program, must be used to protect Internal Use Only information.

Asset Management:

- Company ABC information should be completely removed from wireless hand-held devices that are sent in for repairs and maintenance, or where ownership is transferred.

Acceptable Use:

- Wireless hand-held devices must be used in accordance with the Acceptable Use Policy, and associated standards and guidelines.

Threat Assessment and Monitoring:

- The theft or loss of wireless hand-held devices that transmit, store or originate Company ABC information constitutes a security incident and should be reported in accordance with the Threat Assessment and Monitoring Policy and associated standards and guidelines.

Additional Guidance

The follow Company ABC-approved programs can be installed:

- Certicom Secure Memo Pad
- Pimlico DateBk4
- Timesheet

Appendix C -- Web-Based Policy Distribution

An important step in substantively reducing an organization's risks involves communicating the Information Security policy and providing appropriate education and training for new hires, employees and third parties such as contractors, partner and consultants. This is reflected in the META Security Group Information Security Policy Framework through the Security Awareness Policy that mandates a formal Security Awareness Program. In addition to facilitating awareness of the Information Security Program Charter and associated policies, standards, guidelines and procedures, an organization must develop a distribution system to ensure current policy information is easily available to those who need to access it. META Security Group recommends that organizations leverage Web-based, Intranet solutions to manage and distribute security policy information throughout the organization.

Currently, many organizations use binders and other hardcopy formats to distribute policy information. These policy documents are distributed to each individual or are accessible through the binders or hardcopies stored on the bookshelves of Human Resources or management. In other situations, organizations have distributed policy information through electronic documentation such as electronic mail, and files stored on CDs or floppies. When using these methods, organization face the following problems:

- **Document Version Control:** It is difficult to ensure that individuals have the most up-to-date information with physical and some electronic distribution schemes. Even if the documents are electronically distributed, having multiple copies circulating throughout the organization ensures out-of-date information will be available and referenced.

- **Difficult to Use:** Many policy documents, in both printed and electronic formats, tend to be large and cumbersome. End users must navigate through vast amounts of information to find what they need or understand what applies to them. In many situations, the "typical" employee only needs to read and understand a fraction of the overall policy documentation set. While well-structured electronic documents with a clear table of contents and hyperlinks can improve the end-user experience, the document version control issues discussed above remain problematic.

- **Distribution Costs**: The price of printing and distributing physical documents throughout the organization can be prohibitive. While the policies should not change often, the various standards and procedure do. While printing and distributing the policy document set once may not be too costly, the typical update cycles can become burdensome.

A Web-based, Intranet policy distribution solution not only addresses the aforementioned problems but also provides the following benefits:

- **Timeliness of New Policy Framework Information:** A single up-to-date source such as an Intranet site can ensure new policy information is available immediately. Electronic and paper-based announcements can be sent to individuals to highlight changes or additions to policy or related information located on the Intranet site (for example, an e-mail announcement with a description and link to the new or updated information on the Intranet site).

- **Enforceability:** While ignorance of the law does not excuse violations of it, the same is not always true for an organization's security policy. Enforceability of security policy is somewhat more complicated. Many jurisdictions require an organization to demonstrate that employees were apprised of the security policy and had easy access to it. An organization can provide ongoing awareness, as well as improve accountability and enforceability, by placing the company policy information in a central, easy-to-access Intranet site.

- **Role-based Access:** In general, unauthorized access to security policy information does not necessarily pose a security risk. However, more sensitive policy framework elements must be protected. For example, the incident response standards and procedures should only be provided to a limited number of individuals or groups in the organization. Through the use of role-based access controls, a Web-based, Intranet solution allows the more effective management of access to policy documents. Roles can be defined for individuals or various groups such as end-users, management, consultants, or members of the Security Incident Response Team.

- **Integration and Linkages**: A Web-based, Intranet solution allows further integration and linkage among related policy documents, as well as other related security sources. For example, organizations will find the following links particularly useful in their policy document set:

    - Links between framework elements where policies are linked to standards, which are in turn linked to procedures. The organization can maintain the business linkages established in the top-level policies down at the procedural level.
    - Links to various processes referenced in the policies such as exception handling and change control.
    - Links to internal and external training material.
    - Links to other corporate policy information such as Code of Ethics or regulatory documents.

Organizations have already leveraged Web-based, Intranet technologies in numerous situations that require information and documents to be communicated and accessed throughout the organization. In a similar manner, a Web-based, Intranet policy delivery

solution provides an extremely useful and cost-effective way to manage and distribute policy information.