OrgName
Policy

Identifier:	**xxx**	Revision #:	**0.00**
Superceded Id:	**None**		
Title:	**Framework for Policies, Practices, & Procedures in Security and Compliance**		
Approved by:(signature)		Date (ccyymmdd)	
Approved by (text):	**xxx**		
Approver (title):	**xxx**		
Retirement Date:	**Active**		

Purpose:

To provide ***OrgName*** management with guidance regarding the creation and maintenance of policies, practices, and procedures concerned with security.

Policy:

Table of Content

Notice:
This is a living document. It should be referred to frequently for updates, especially updates to the values defined in appendices. Its publicly available location is: ***PolicyLocation***.

I. Summary:

The ***OrgName*** has and needs security oriented policies that are implemented as a hierarchy of policies, practices, and procedures, with policies being the root. Policies are created, championed, and approved by the upper levels of ***OrgName***'s management structure, while practices and procedures, based on policies, are the domain of lower levels of management. Policies are the most general statement on a subject and procedures are the most specific. Policies generally set ***OrgName***'s goals, practices specify a general means of achieving the goals, and procedures are filled with action specifications on how to reach the goals in an everyday work environment.

The remainder of this document will enlarge on these concepts and how they produce a coherent policy framework.

II. Structure:

This document is intended to specify a framework that will assist ***OrgName*** in creating and organizing its security oriented policies, practices, and procedures (hereafter just policies, practices and procedures or PPPs), in a manner that meets ***OrgName***'s data security requirements.

Structurally ***OrgName***'s policies, practices, and procedures are implemented as a hierarchy of authority and specificity. This hierarchy is rooted at ***OrgName***'s "C" level (.i.e. the CIO and direct reports), and extends through the management of individual units. In general the detail increases as authority, authorship, and approval occur at lower levels of the organization.

Policies are statements specifying the goals of ***OrgName***'s security functions. These goals, when met collectively, place ***OrgName*** in compliance with ***OrgName***'s regulatory… security requirements. Policies are the foundation upon which practices and procedure may be built. The questions to keep asking regarding policies are;

- do the policies provide appropriate guidance for the creation of practices and procedures, and
- are their goals met via the practices and procedures implemented because of the policies?

Practices are statements specifying the manner in which the goals, specified in the policies, are to be met. Practices attempt to take the policies, somewhat subjective in nature, and place them into a more measurable objective context. Two questions should be continually ask regarding practices;

- first do the practices attain the goals set out in the policies, and
- second do the procedures implementing practices actually meet the objects specified in the practices.

Procedures are statements specifying the means by which practices are implemented. Procedures attempt to define actions ***OrgName*** should take in implementing the practices in order to achieve their objectives. Unlike a policy or practices, which address needs in relatively general terms, a procedure is filled with action statements that specify exactly and concretely how objectives are to be met. Procedures could be part of the daily operations manual for the organization.

Figure 1 illustrates the preceding relationships.

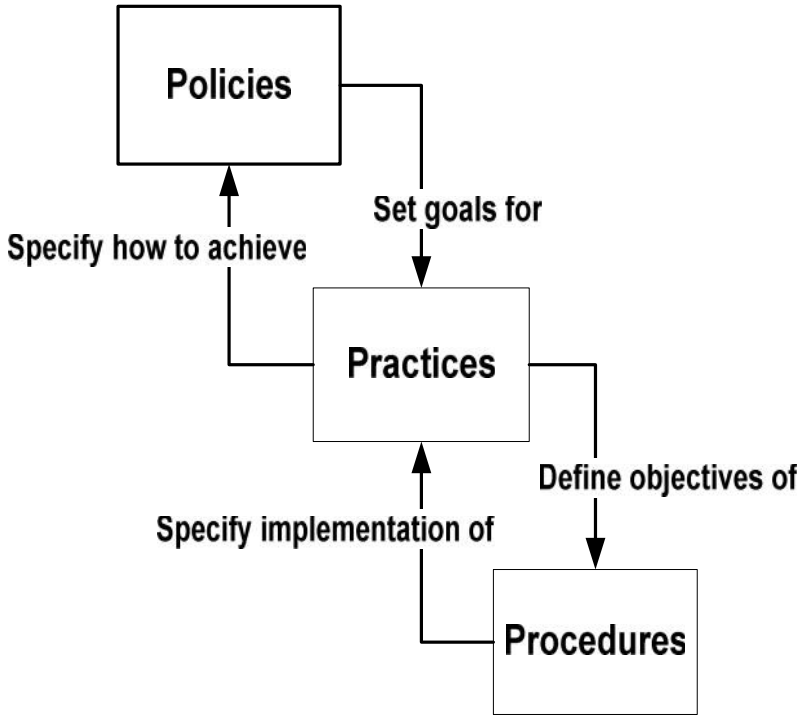

Figure 1 - Hierarchy of Policies, Practices, and Procedures.

Not explicit in either the description or figure is the relative volume or life of these statements. In most situations the volume of each can be represented by:

Number of Policies <= Number of Practices <= Number of Procedures

That is, the closer to actual implementation, the more detail must be covered and therefore the more practices/procedures are needed. The worst case is of course when the number of policies, practices, and procedures are the same – an unlikely occurrence.

Similarly, the closer to implementation, the shorter the life expectancy as represented below:

Life of Policies >= Life of Practices >= Life of Procedures

It is to be expected that in a technical environment the means of attaining an objective or goal (satisfying a practice and or policy) will change more often than the objective or goal itself Again the worst case is when the age of all three (3) is the same.

These relationships should help ***OrgName*** remain stable through expected evolutionary changes. Changes such as technologies, personnel, and relationships with outside organizations are more likely to impact the more specific aspects than the more general. So expect procedures and maybe practices to change in reaction to evolutionary changes, but policies should remain stable. While this structure is likely to insulate policies, and possibly practices, from evolutionary changes, it is unlikely that any structure will insulate policies from revolutionary changes.

Along with stability this hierarchical approach provides four (4) vital aspects of the policy implementation process;

the ability of ***OrgName***'s upper levels of management to champion, approve, promulgate, and support policies while not being overwhelmed with detail,

the ability to define policies, practices, and procedures iteratively, thus allowing personnel with the appropriate level of knowledge to be tasked with assisting authorship and implementation,

flexibility where practices and procedures may vary in detail as needed to achieve policy goals in different organizational units, and

the ability of anyone with ***OrgName*** to obtain policy driven guidance at an appropriate level of language and detail.

Caveat:

While this organization for policies/practices/procedures provides several advantages there may be times when a less hierarchical approach makes more sense. This organization is considered best in most circumstances but policy/practice/procedure authors should proceed as is best for ***OrgName***'s operations.

III. Identification Protocol:

Being able to identify a policy/practice/procedure, be that forward identification (policy to practice to procedure) or reverse identification (procedure to practice to policy) makes entire policy structure more useful and comprehension easier. To facility identification each policy/practice/procedure is to be labeled with a structured identifier that will assist readers in understanding its relationship to others.

Like the relationship between policies, practices, and procedures, the identifiers are hierarchical in nature. The components of the identifier are:

Place OrgName specific details on an Identifier structure here.

IV. Presentation:

Physical presentation of a policy/practice/procedure is largely at the author's discretion. However there is a suggested format for use when there is no overriding reason for a different format. This format is displayed in **Appendix X – Presentation**, and available as a Template.

Place details on presentation into appendix x in whatever template form is appropriate.

V. Approval:

Place details of where within OrgName's organizational structure PPPs need to be approved.

Approval is obtained by having the appropriate position sign and date a hardcopy of the statement.[1] The signed and dated copy should then be forwarded to the ***appropriate-staff*** for preservation and publication.

VI. Maintenance and Archiving:

The maintenance and archiving of policies/practices/procedures is the responsibility of the incumbent ***appropriate-staff-position*** *(if this position is unavailable the* ***appropriate-C-Suite-staff*** *should assign the responsibility to another position within the* ***OrgName****)*. This responsibility includes, but is not limited to, the following:

Assuring the original hardcopy, with approval signature, of the policy/practice/procedure is secured in the ***OrgName***'s document library.

Maintaining an ***OrgName*** internally visible electronic reference site for approved and proposed policies/practices/procedures, with the distinction between proposed and approved status easily discerned.[3]

Maintaining an ***OrgName*** internally visible source of document templates and other tools for producing and maintaining policies/practices/procedures.

Maintaining the master list of assigned policy/practice/procedure identifiers, their associated titles.

Assigning identifiers for new/proposed policies/practices/procedures.

[1] A goal is to have the approval use digital signatures instead of physical signatures. This will enhance the ability to preserve and publish the statements.

VII. History:

Each policy/practice/procedure should contain as its last content a revision history of itself. Each time modification occurs and the modification is semantically significant, that is more than just spelling, grammar, or presentation, an entry in the history table should be added. Revisions should be presented in reverse chronological order, i.e. newer history entries should be toward the top of the history table. The information in the table should, at a minimum, be:

Date	the date on which the modification was made
Author(s)	the person that made the modification
Section(s)	the section(s) of the document that was affected
Type(s)	the type of modification; A – for addition, D – for deletion, M – for modification
Revision(s)	the revision numbers applied to the statement. Revisions should have origin 0 and be of the form 0.00 for the initial version. If a change, i.e. addition, deletion, or modification has no impact on the meaning of the statement then a revision number change need not be made. If the impact on meaning is considered minor the number should be incremented by 0.01. In cases where the impact is considered to be major the number should be changed to the next largest whole number, e.g. if revision 1.03 underwent significant modification its number would be promoted to 2.00.
Description	a short description of the modification

See ***Appendix X – Presentation*** for a history table in the policy/practice/procedure template.

VIII. Appendix A – A Policy/Practice/Procedure Example:

The following three (3) subsections are abbreviated examples of content for a policy, practice, procedure hierarchy. The example addresses the disposal of electronic storage media no longer needed or being repurposed.

A. Policy:

Disposal of Electronic Storage Media:

Electronic storage media may be disposed of by destruction or transfer to another entity.

1. Transfer:

   Disposal by transfer is the disruption of all resident data beyond any reasonable means of recovery, followed by physical and ownership transfer to another entity. See policy x on transfer of hardware.

2. Destruction:

   Disposal by destruction is the permanent disruption of the media's usability beyond any reasonable means of data recovery.

B. Practices:

Disposal of Electronic Storage Media:

Electronic storage media that is erasable may be disposed of by destruction or transfer.

Electronic storage media that is not erasable may only be disposed of by destruction.

1. Transfer of Erasable Electronic Storage Media:

   Electronic storage media that is erasable, e.g. magnetic media and optical media that is rewritable, may be transferred to another entity by:

   1) Erasure/destruction of all resident data, by the technology appropriate means, beyond any reasonable means of recovery.
   2) If the media has a unique identifier, e.g. serial number, log the erasure/destruction of the resident data.
   3) If necessary, e.g. to account for residual value, prepare transfer of ownership documentation.
   4) Physically transfer media to new owner.

2. Destruction of Erasable or Non-erasable Electronic Storage Media:

   Electronic storage media that is erasable, e.g. magnetic media, or not erasable, e.g. write once optical media, may be destroyed by:

   1) If the media is un-mounted, e.g. magnetic tape, diskette, optical CD, etc., destroy the physical integrity of the media such that reassembly for use may not be accomplished by reasonable means.
   2) If the media is mounted, e.g. Winchester disk drives, disassemble the mechanism and destroy the exposed media as if it were un-mounted media.
   3) If the media has a unique identifier, e.g. serial number, log the destruction.

C. Procedures:

Disposal of Electronic Storage Media:

1. Transfer of Erasable Electronic Storage Media.

   Microsoft Windows Media

   1) Mount media in a stand-alone Intel Processor environment.
   2) Boot machine with OnTrack disk eraser.
   3) Erase mounted media.
   4) Unmount media
   5) If the media being transferred is a Winchester technology hard disk; log into facility network with an ID having access to media inventory server, open transfer log located at \\Server\MountPoint\Logs\TransferLog, enter disk serial number into log as being erased along with destination of transfer.
   6) Transfer disk to destination.

2. Destruction of Erasable or Non-erasable Electronic Storage Media:

   Unmounted Media, e.g. tapes or diskettes

   1) Remove tape from reel/cassette or diskette from slip cover.
   2) Pass exposed media through shredder producing residual less than 0.25” square.
   3) Place shredded media into non-medical / non-incinerated trash.

History:

Date (yymmdd)	Author	Section-Type(A – add, D – delete, M – mod)	Rev #	Description
yymmdd	Surname, GivenName	All - A	0.00	Initial publishing