Development of Information Labeling Standard

By Malcolm E. Palmer
Edward P. Moser

Copyright Notice

META Security Group
20464-A Chartwell Center Drive, Cornelius, NC 28031
704 895 0837 fax: 704 895 8165
www.metasecuritygroup.com

Printed in the United States of America.

Warning and Disclaimer

No part of this publication shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from META Security Group™. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, META Security Group (publisher and author) assumes no responsibility for errors or omissions. Neither is any liability assumed for damages resulting from the use of the information contained herein.

Table of Contents

1 Introduction

This research report from META Security Group*, Development of Information Labeling Standard*, provides best practices guidance that organizations can reference and leverage to assess, improve, or develop an Information Labeling Standard. The Information Labeling Standard should provide specific instructions and requirements for labeling information assets. 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.

1.1 Audience

There are two primary audiences for this report:

1. Organizations that have implemented or are planning to implement the META Security Group Information Security Policy Framework.

2. Members of Information Security teams.

In addition, this report can be useful to executive management and business unit owners. These individuals can use or reference the report to provide a common understanding of key considerations for an Information Labeling Standard and to enhance communication of an overall Policy Framework.

This report assumes a certain level of understanding of the META Security Group Information Security Policy Framework and terminology, as well as a basic, but not necessarily in-depth, comprehension of information labeling approaches. Section 1.2 of this paper provides a high-level overview of the META Security Group Information Security Policy Framework. Refer to the *META Security Group Information Security Policy Framework* research report for more detailed and comprehensive information.

1.2 Background and Context

As shown in Figure 1, the META Security Group Information Security Policy Framework (the Framework) consists of a hierarchical structure that includes:

- An Information Security Program Charter at the top of the hierarchy that empowers all activity within the Information Security Program.

- Seven policies that further define the Information Security objectives in a number of topical areas.

- Key standards that provide more measurable ("auditable") guidance in each policy area.

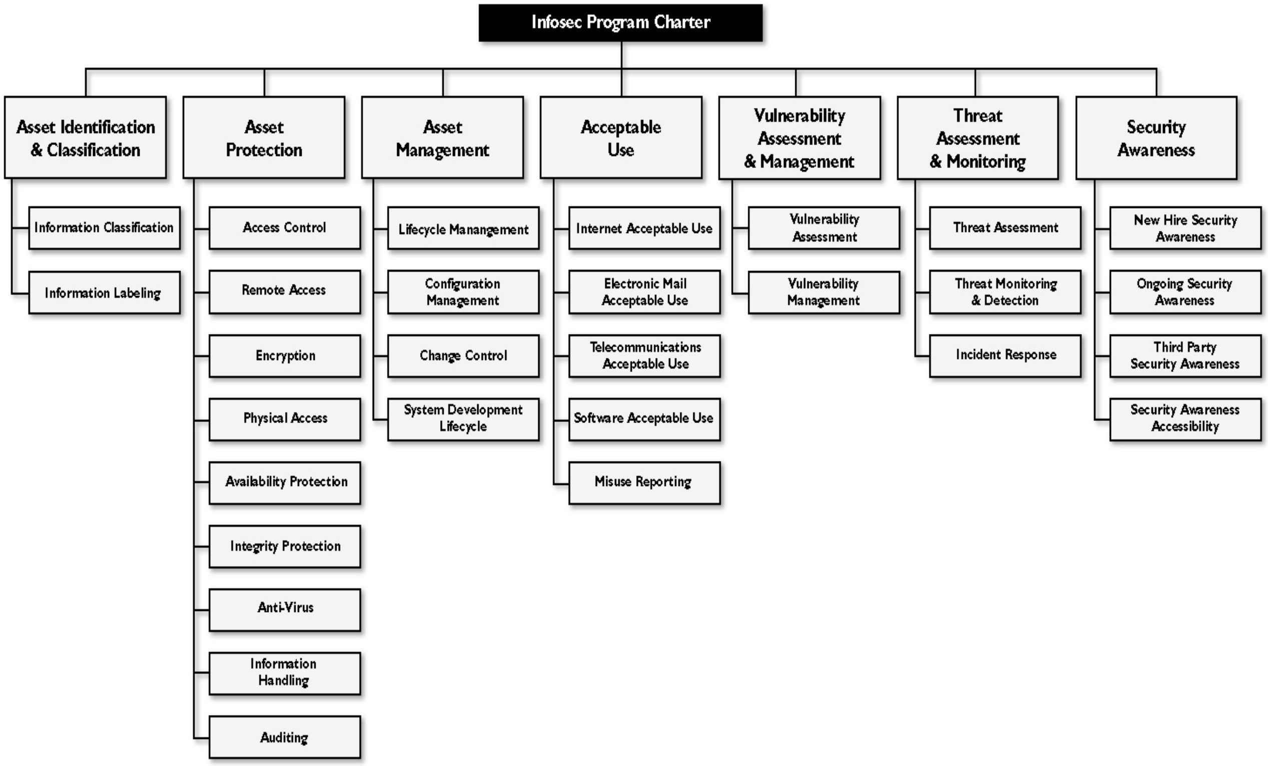

Figure 1: The META Security Group Information Security Policy Framework

This hierarchical structure ensures that the elements at lower levels in the Framework such as standards are referentially associated with the risk management approach and traceable back to the objectives established at the Framework's Security Program Charter and policy levels.

META Security Group has significant experience in developing customized standards for numerous organizations across multiple vertical markets. Our experience suggests that several organization-specific factors must be considered when developing standards. This paper identifies these factors, and outlines a structure for the Information Labeling Standard that is traceable and consistent with the Framework.

1.3 Document Organization

The Key Considerations section discusses specific factors that organizations should consider when developing the Information Labeling Standard.

The Sample Information Labeling Standard section outlines a sample standard established on the basis of the key considerations discussed in the report.

2 Key Considerations

META Security Group has found through its extensive experience with clients that an Information Security standard within the Framework should contain the following major components:

- Purpose Statement
- Scope Statement
- Terms and Definitions
- Requirements
- Responsibilities
- Enforcement and Exception Handling
- Review and Revision Expectations

Sections 2.1 to 2.7 discuss key considerations for each major section of the Information Labeling Standard.

2.1 Purpose Statement

As defined in the META Security Group Information Security Policy Framework, a standard provides more measurable criteria for satisfying and supporting the high-level objectives defined and authorized by the policies. In order to maintain the traceable framework hierarchy, the purpose statement for the Information Labeling Standard should derive from the *Asset Identification and Classification Policy* (see Figure 1).

The *Asset Identification and Classification Policy* defines the objectives for establishing specific standards and guidelines on the identification, classification, and labeling of information assets. The Information Labeling Standard builds on these policy objectives by providing specific instructions and requirements for labeling sensitive information assets. While many organizations focus only on labeling printed information, our extensive experience suggests that a comprehensive approach to information labeling addresses both printed and electronically stored information.

2.2 Scope Statement

The scope of a standard defines to whom the standard applies (for example, all employees, full-time employees only, contractors, consultants, or customers). The scope statement for the Information Labeling Standard should reiterate the scope statement from the *Asset Identification and Classification Policy.*

2.3 Terms and Definitions

The Information Labeling Standard introduces new terms and corresponding definitions. In addition, this standard should restate or reference terms that were previously defined in the charter or policies. The following key terms and definitions are among those that should be defined, restated, or referenced:

- **Asset Custodian or Custodian** – Should restate the definition provided in the *Asset Identification and Classification Policy*.

- **Asset Owner or Owner** – Should restate the definition provided in the *Asset Identification and Classification Policy*.

- **Confidentiality Classifications** – Should reference the definitions in the *Information Classification Standard.*

- **Exchangeable Media** – Should provide a definition that refers to specific examples such as diskettes, tapes, etc.

- **Information Assets** – Should restate or reference the definition in the *Asset Identification and Classification Policy*.

- **Sensitive Information** – Should provide a definition for information that has been classified as Restricted, Confidential, and Internal Use Only.

- **User** – Should restate the definition provided in the *Asset Identification and Classification Policy*.

2.4 Requirements

Many organizations have implemented comprehensive information classification schemes that include confidentiality, integrity, and availability classifications. The Information Labeling Standard should provide specific instructions and requirements for labeling an information asset based on its sensitivity or confidentiality classification.

The following sections cover labeling requirements relating to printed and electronically stored information.

2.4.1 Printed Information

The labeling requirements for printed information should clearly state how printed sensitive information must be labeled or marked. These labeling requirements, at a minimum, should provide specific markings for the cover or title page, as well as the headers and footers for each page of the printed document. For clarity, the requirements should be provided in a tabular format.

2.4.2 Electronically Stored

The labeling requirements for electronically stored information should clearly state how sensitive information stored on exchangeable media must be labeled or marked. These labeling requirements, at a minimum, should provide specific markings for the external labels and electronic labels.

2.5 Responsibilities

The Information Labeling Standard should assign, to members of the organization, the responsibilities for meeting the requirements. These responsibilities also should expound on and be consistent with the responsibilities outlined in the *Asset Identification and Classification Policy*. Moreover, the responsibility assignments should be consistent with the *Information Security Program Charter*. Table 1 identifies typical responsibilities and assignments associated with this standard.

Responsibilities	**Typically Assigned to**
Approves the standard.	Chief Information Security Officer
Develops and maintains the standard.	Chief Information Security Officer
Ensures compliance to the standard.	Chief Information Security Officer Information Security Department or Team
Ensures proper labeling.	Owner
Ensures labeling requirements are communicated and understood.	Owner
Maintains and conserves the labels.	Custodian User
Contacts the Owner, when information is unmarked or labeled improperly.	Custodian User

Table 1: Responsibilities and Assignments

2.6 Enforcement and Exception Handling

The Information Labeling Standard should reiterate or expound upon the enforcement statement established in the *Asset Identification and Classification Policy*. The exception handling statement should reference an existing procedure or outline specific steps for requesting and submitting an exception to the standard. In addition, the exception handling statement should reiterate the need to comply with the current standard while exception requests are under consideration.

2.7 Review and Revision Expectations

The Information Labeling Standard should reiterate or expound upon the review and revision statements established in the *Asset Identification and Classification Policy*.

3 Sample Information Labeling Standard

This section outlines a sample Information Labeling Standard that is consistent with the Framework and incorporates the key considerations discussed in the body of this report.

Sample Information Labeling Standard

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

This *Information Labeling Standard* builds on the objectives established in the *Asset Identification and Classification Policy*, and provides specific instructions for labeling sensitive information assets. These instructions address labeling requirements for printed and electronically stored information.

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 (the "Company") information or systems, are covered by this standard and must comply with associated guidelines and procedures.

Information assets are defined in the *Asset Identification and Classification Policy*.

Confidentiality classifications are defined in the *Information Classification Standard*.

Exchangeable media refers to diskettes, tapes, removable hard drives, compact disks or CD, etc.

Sensitive information refers to information that has been classified as Restricted, Confidential, or Internal Use Only.

II. Requirements

A. Printed Information

1. All printed sensitive information must be appropriately labeled or marked to indicate its confidentiality classification.

   The appropriate labels for cover/title pages and headers or footers are provided in the following table:

Confidentialit y Classification	Cover/Title Page Label	Header or Footer Label (each page)
Restricted		
Confidential		
Internal Use Only		

B. Electronically Stored Information

1. All exchangeable media that stores sensitive information must be appropriately labeled or marked to indicate its confidentiality classification.

   The appropriate external and electronic labels are provided in the following table:

Confidentialit y Classification	External Label	Electronic Label (if available)
Restricted		
Confidential		
Internal Use Only		

III. Responsibilities

The Chief Information Security Officer (CISO) approves the *Information Labeling Standard*. The CISO also is responsible for the development, implementation, and maintenance of the *Information Labeling Standard*.

The individuals, groups, or organizations identified in the scope of this standard are accountable for one or more of the following levels of responsibility when using Company 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 ensuring the proper labeling of sensitive information, and ensuring the information labeling requirements for electronically stored and printed information are properly communicated and understood by the Custodians and Users.

- 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 labeling requirements; applying the necessary controls, in accordance with the *Asset Protection Policy*, to maintain and conserve the established information labels; and contacting the Owner when sensitive information is unmarked or labeled improperly.

- Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for familiarizing themselves with the *Information Labeling Standard* and associated guidelines and procedures; maintaining and conserving the established information classification and labeling; and contacting the Owner when sensitive information is unmarked or labeled improperly.

IV. Enforcement and Exception Handling

Failure to comply with the *Information Labeling Standard* and associated 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 *Information Labeling Standard* should be submitted to <Insert Title> in accordance with the *Information Security Standards Exception Procedure*. Prior to official management approval of any exception request, the individuals, groups, or organizations identified in the scope of this standard will continue to observe the *Information Labeling Standard.*

V. Review and Revision

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

Approved: ____

Signature
<Insert Name>

Chief Information Security Officer