Development of Information Classification Standard

By Malcolm E. Palmer
Edward P. Moser

Copyright Notice

Scalable Software
2929 Allen Parkway, Suite 1400 Houston, TX 77019
713.316.4900 fax: 713.316.4975
www.scalable.com

Printed in the United States of America.

Warning and Disclaimer

Table of Contents

1 Introduction

This research report from Scalable Software*, Development of Information Classification Standard*, provides best practices guidance that organizations can reference and leverage to assess, improve, or develop an Information Classification Standard. The Information Classification Standard should provide specific instructions and requirements for classifying, reclassifying, and declassifying information assets. The insights provided in this report are derived from the considerable "real world" experience gained by Scalable Software 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 Scalable Software 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 Classification Standard and to enhance communication of an overall Policy Framework..

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

1.2 Background and Context

As shown in Figure 1, the Scalable Software 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.

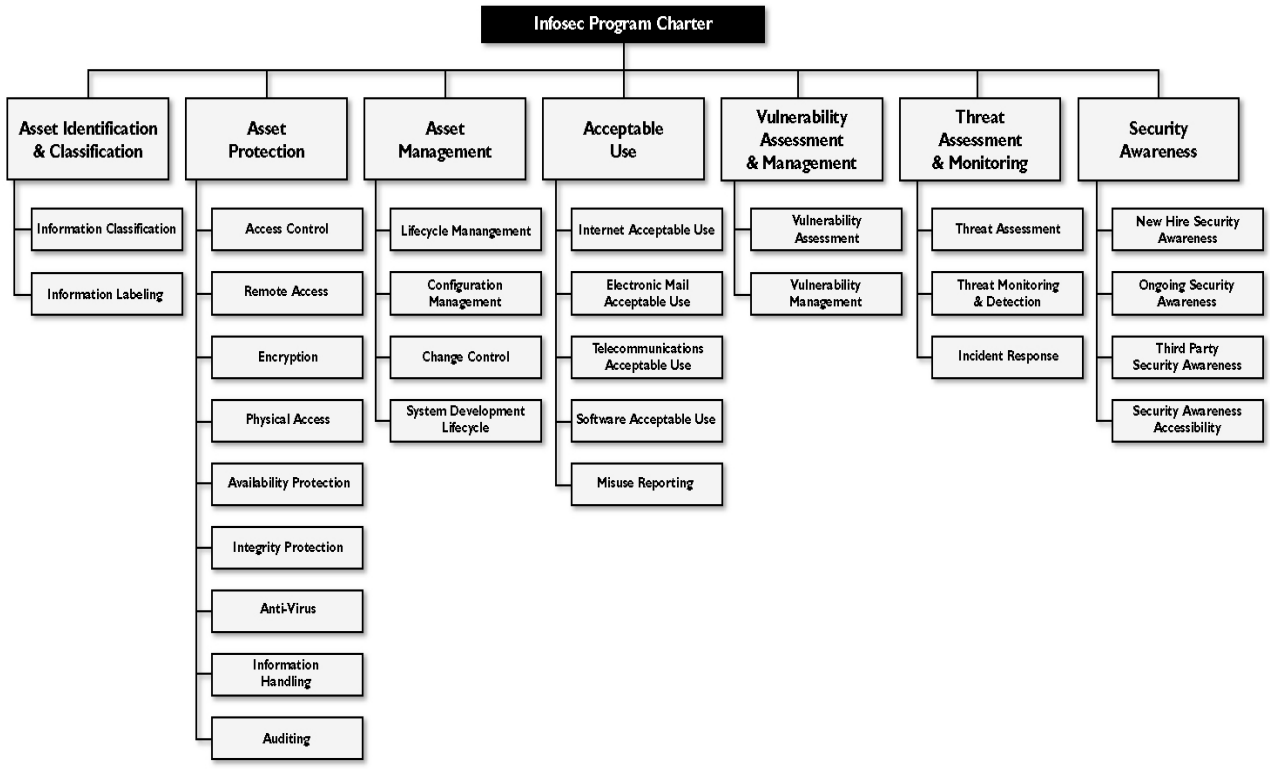

Figure 1: The Scalable Software Information Security Policy Framework

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.

Scalable Software 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 Classification 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 Classification Standard.

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

2 Key Considerations

Scalable Software 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 Classification Standard.

2.1 Purpose Statement

As defined in the Scalable Software 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 Classification 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 Classification Standard builds on these policy objectives by providing specific instructions and requirements for classifying information assets. While many organizations focus only on the confidentiality of information assets, our extensive experience suggests that a comprehensive approach to information classification addresses confidentiality, integrity, and availability.

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 Classification Standard should reiterate the scope statement from the *Asset Identification and Classification Policy.*

2.3 Terms and Definitions

The Information Classification 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*.
- **Availability** – Should provide a definition that refers to ensuring the availability of information assets.
- **Confidentiality** – Should provide a definition that refers to protecting sensitive information assets.
- **Information Assets** – Should restate or reference the definition in the *Asset Identification and Classification Policy*.
- **Integrity** – Should provide a definition that refers to ensuring the auditability and reproducibility of information assets.
- **User** – Should restate the definition provided in the *Asset Identification and Classification Policy*.

2.4 Requirements

The Information Classification Standard should provide specific instructions and requirements for classifying, reclassifying, and declassifying information assets.

The following sections cover classifications relating to confidentiality, integrity, and availability.

2.4.1 Confidentiality Classifications

The confidentiality classification requirements should provide detailed descriptions and specific examples for the confidentiality classifications (for example, Restricted, Confidential, Internal Use Only, Public) established at the policy level (that is, in the *Asset Identification and Classification Policy*). For clarity, the descriptions and examples should be provided in a tabular format. In addition, the confidentiality classification requirements should address "proprietary" information that is shared outside the organization but where the organization

retains ownership of the information. Third party information for which the organization has a custodial role, as well as default parameters for information that has not been explicitly classified, should also be addressed.

The *Asset Identification and Classification Policy* states that, at a minimum, "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.[1]" The confidentiality classification requirements should expound on this policy objective and provide specific instructions for each instance. For example, a confidentiality classification scheme that consists of Restricted, Confidential, Internal Use Only, and Public categories should address each of the following instances:

- Restricted information combined with Confidential, Internal Use Only or Public information
- Confidential information combined with Internal Use Only or Public information
- Internal Use Only information combined with Public information

2.4.2 Integrity Classifications

Some organizations have established information classification approaches at the policy level that include integrity objectives in which certain information asset are classified as Integrity Protected. This classification indicates that the information, in electronic form, should be protected by data inspection or other techniques (for example, MD5, CRC checksum, etc) to detect or prevent data tampering.

The integrity classification requirements should outline the criteria and provide specific examples for the Integrity Protected classification. Specific data inspection techniques are addressed in the *Integrity Protection Standard*.

2.4.3 Availability Classification

Some organizations have established information classification approaches at the policy level that include availability objectives. These organizations typically have established Information Security Programs that integrate business continuity and recovery objectives at the security charter and policy levels to help the organization define availability requirements.

---

[1] Note that some combinations of information may require a classification even more restrictive than any individual component. For example, a report that consolidates Confidential information from a number of departments may be classified as Restricted because the aggregated information, considered in its entirety, meets the definition of Restricted information.

The availability classification requirements should provide detailed criticality and outage descriptions. They also should provide examples for the availability classifications (for example, High, Medium, Low) established at the policy level (that is, in the *Asset Identification and Classification Policy*). Descriptions of criticality and tolerance for loss or outages should be consistent with the organization's existing business continuity and recovery plans. For clarity, the descriptions and examples should be provided in a tabular format.

2.4.4 Reclassification and Declassification

Information may progress through several classification categories. For example, press releases or announcements may start as Restricted information (when first drafted), but eventually become Public when publicly announced by an authorized representative. While the policy establishes "periodic" reviews, the reclassification requirements should specify the frequency at which information should be reviewed to determine if the information classification should be changed. In addition, the Information Classification Standard should specify any automatic declassification instructions or requirements.

2.5 Responsibilities

The Information Classification 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
Assign proper classification.	Owner
Ensures classifications are communicated and understood.	Owner
Ensures reviews of classification.	Owner
Applies, maintains, and conserves the	Custodian

classification.	User (only maintains and conserves)
Contacts the Owner, when the classification is unknown.	User

Table 1: Responsibilities and Assignments

2.6 Enforcement and Exception Handling

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

3 Sample Information Classification Standard

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

Sample Information Classification 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 Classification Standard* builds on the objectives established in the *Asset Identification and Classification Policy*, and provides specific instructions for classifying information assets. These instructions include Confidentiality, Integrity, Availability information classification requirement as well as reclassification and declassification requirements.

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 refers to protecting sensitive information assets.

Integrity refers to ensuring the auditability and reproducibility of information assets.

Availability refers to ensuring the availability of information assets.

II. Requirements

A. CONFIDENTIALITY

1. All Company information shall be classified in one of four confidentiality categories:

    - Restricted
    - Confidential
    - Internal Use Only
    - Public

    A description of each category is provided in the following table:

Confidentiality Classification	Description	Examples
Restricted	Information, the unauthorized disclosure of which would: <Insert company-specific description>	Examples may include: <Insert company-specific examples>
Confidential	Information, the unauthorized disclosure of which would: <Insert company-specific description>	Examples may include: <Insert company-specific examples>
Internal Use Only	Information confined to use only within Company ABC for purposes related to its business.	Examples may include: <Insert company-specific examples>
Public	Information and material to which access may be granted to any other person or organization.	Examples may include: <Insert company-specific examples>

2. The generic term "proprietary" will be used to refer to specific instances of Restricted, Confidential, and Internal Use Only information to indicate the proprietary nature of Company information that may be shared outside the Company, but where the Company retains ownership of the information.

3. Third party proprietary business data, for which Company has a custodial role, will be classified with the appropriate category plus "Company XYZ Proprietary" (e.g., Company Confidential and Company XYZ Proprietary).

4. When information has not been explicitly classified as Restricted, Confidential, or Internal Use Only, the information by default shall not be considered as Public.

5. When Restricted information is combined with Confidential, Internal Use Only or Public information, the resulting collection of information must be classified as Restricted.

6. When Confidential information is combined with Internal Use Only or Public information, the resulting collection of information must be classified, at a minimum, as Confidential.

7. When Internal Use Only information is combined with Public information, the resulting collection of information must be classified, at a minimum, as Internal Use Only.

B. INTEGRITY

1. The Integrity Protected classification indicates that the information, in electronic form, should be protected by Company-approved encryption or data inspection techniques that ensure the information has not been intentionally or inadvertently altered. Refer to the *Integrity Protection Standard* for specific instructions and information on Company-approved data inspection and other techniques for achieving Integrity protection objectives.

2. The Integrity Protected classification shall be applied with discretion to an information asset that if accidentally or intentionally altered without authorization would significantly damage the Company's competitive advantage and reputation or could lead to legal liabilities.

   Possible examples of Integrity Protected information include:

   <Insert company-specific examples>

C. AVAILABILITY

1. All Company information shall be classified in one of three availability categories:

   - High
   - Medium
   - Low

   A description of each category is provided in the following table:

Availability Classification	Description	Potential Loss or Impact
High	High to continuous availability required. <Insert company-specific description>	Serious to severe impact. Examples may include: <Insert company-specific examples>
Medium	Standard availability required.	Limited to serious impact. Examples may include:

Availability Classification	Description	Potential Loss or Impact
	<Insert company-specific description>	<Insert company-specific examples>
Low	Limited availability required. <Insert company-specific description>	No critical impact. Examples may include: <Insert company-specific examples>

D. RECLASSIFICATION

1. Restricted information shall be reviewed for reclassification by the Asset Owner on a specific review date not to exceed <#> years.

2. Confidential and Internal Use Only information shall be reviewed annually for reclassification. In accordance with Company procedures, this review may be conducted sooner in response to specific requests for reclassification.

E. DECLASSIFICATION

1. Restricted information shall be automatically declassified after <#> years.

2. Declassification shall be performed in accordance with Company procedures.

III. Responsibilities

The Chief Information Security Officer (CISO) approves the *Information Classification Standard*. The CISO also is responsible for the development, implementation, and maintenance of the *Information Classification 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 assigning the proper information classifications; ensuring the information classifications are properly communicated and understood by the

Custodians and Users; and ensuring that information assets are reviewed for reclassification.

- 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 defining and implementing the necessary controls to apply, maintain, and conserve the information classifications established by the Owners.

- Users are the individuals, groups, or organizations authorized by the Owner to access information assets. Users are responsible for familiarizing themselves with the *Information Classification Standard* and associated guidelines and procedures; maintaining and conserving the information classification established by the Owners and applied by the Custodians; and contacting the Owner when the information classification is unknown.

IV. Enforcement and Exception Handling

Failure to comply with the *Information Classification 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 Classification 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 Classification Standard.*

V. Review and Revision

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

Approved: _____

Signature
<Insert Name>
Chief Information Security Officer