Development of Internet Acceptable Use Standard

By Malcolm E. Palmer
Edward P. Moser

Copyright Notice

Scalable Software, Inc.
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

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 Scalable Software, Inc. 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, Scalable Software (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 Scalable Software*, Development of Internet Acceptable Use Standard*, provides best practices guidance that organizations can reference and leverage to assess, improve, or develop an Internet Acceptable Use Standard. The Internet Acceptable Use Standard should provide specific instructions and requirements on the proper and appropriate business use of Internet resources. 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 Internet Acceptable Use 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. 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.

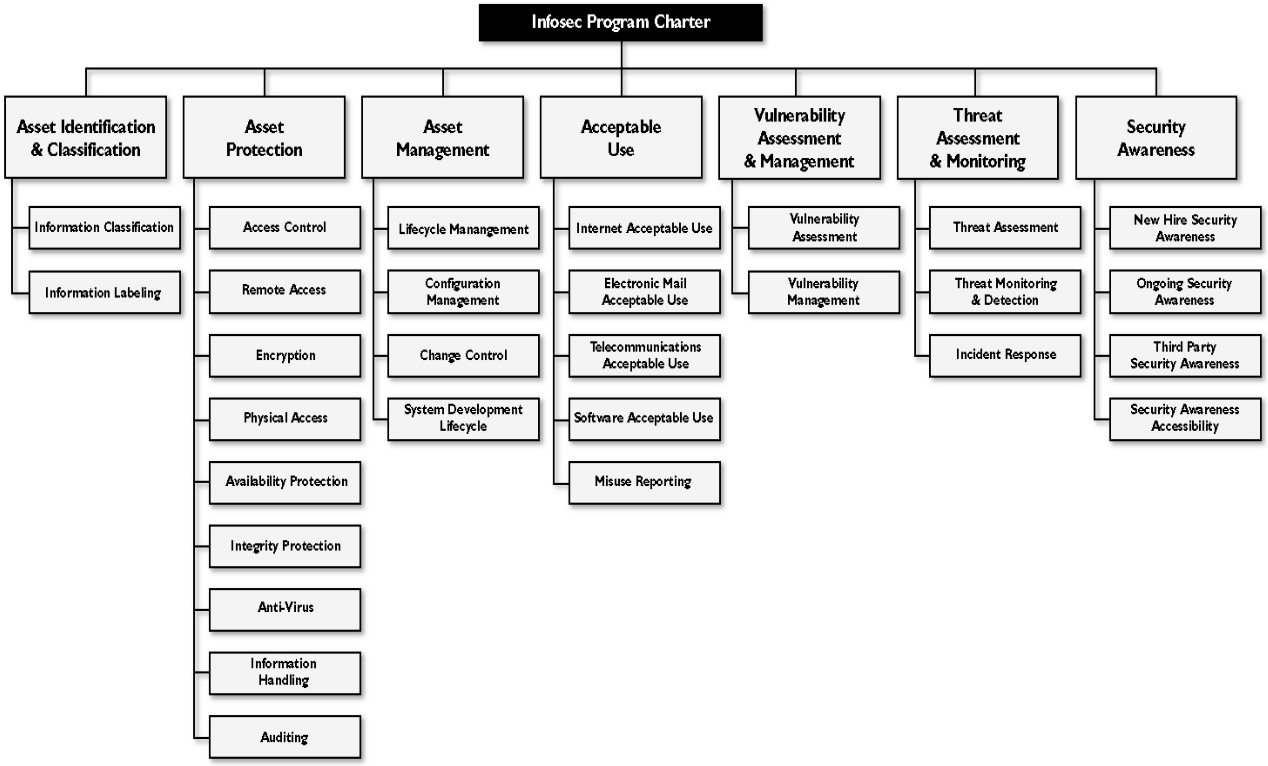

Figure 1: The Scalable Software Information Security Policy Framework

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 Internet Acceptable Use 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 Internet Acceptable Use Standard.

The Sample Internet Acceptable Use 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 Internet Acceptable Use 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 Internet Acceptable Use Standard should derive from the *Acceptable Use Policy* (see Figure 1).

The *Acceptable Use Policy* defines the objectives for establishing specific standards on the appropriate business use of information assets. The Internet Acceptable Use Standard builds on these policy objectives by providing specific instructions and requirements on the proper and appropriate business use of Internet resources.

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 Internet Acceptable Use Standard should reiterate the scope statement from the *Acceptable Use Policy.*

2.3 Terms and Definitions

The Internet Acceptable Use 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:

- **Information Assets** – Should restate or reference the definition in the *Asset Identification and Classification Policy*.
- **Internet Resources** – Should provide a definition that refers to the systems, networks equipment, and software that provide access to and/or use of the Internet.
- **Objectionable** – Should provide a definition that refers to the specific scope of instances or uses that could be considered "objectionable" including, but not limited to, those that are or could be perceived to be obscene, harassing, offensive, or any other uses that would reflect adversely on the organization.
- **Users** – Should provide a definition that refers to the individuals, groups, and organizations that the organization has authorized to access and use its Internet resources.

2.4 Requirements

The Internet Acceptable Use Standard should provide specific instructions and requirements on the proper and appropriate business use of Internet resources. However, it is not possible to develop or list specific requirements for every manner in which Internet resources may be used. The requirements of the Internet Acceptable Use Standard, therefore, should not be considered a comprehensive listing. However, an organization should consider consistency with these requirements as the basis for considering the appropriateness of other activities and practices that are not specifically addressed.

The following sections cover requirements for business use, improper use, browser software and downloaded materials, as well as monitoring rights, privacy expectations, and reporting misuse.

2.4.1 Business Use

Internet use can provide significant business benefit for an organization. However, there are also significant legal, security, and productivity issues related to how the Internet is used. Stating that Internet resources are provided only for business use is both impractical and unenforceable. Business use issues typically are addressed by stating that the Internet resources are provided primarily for business purposes, and by stating specific conditions for limited personal use. In addition, business use requirements should address applicable legal and regulatory compliance, as well as user accountability.

2.4.2 Improper Use

Although organizations may provide Internet resources primarily for business purposes with some limited personal use, there are several types of activities that are inappropriate and improper. The improper use requirements of the Internet Acceptable Use Standard primarily should prohibit the use of Internet resources for activities that are illegal, conflict with business interests, or interfere with productivity and business operations. In addition, these requirements should prohibit accessing, downloading and transmitting objectionable material, as well as personal and non-business solicitations.

2.4.3 Browser Software

Because the type of browser and its configuration can directly expose an organization's information assets, the browser software requirements for the Internet Acceptable Use Standard should primarily restrict users to approved browser software and configurations. In addition, the requirements should prohibit users from changing browser configurations to less restrictive security settings.

2.4.4 Downloaded Materials

Access to the Internet allows users to download software and other materials from the Internet. The software or materials downloaded from the Internet can exploit existing vulnerabilities or introduce malicious code or viruses to the organization's information systems and networks. The downloaded materials requirements for Internet Acceptable Use Standard should prohibit users from downloading unauthorized software. They also should require downloaded materials to be reviewed for malicious code in accordance with established policies and standards.

2.4.5 Right to Monitor

Many organizations deploy monitoring and filtering capabilities (that is, processes and supporting technologies) to determine how Internet resources are used, and to prevent access to objectionable sites and content. In addition, these capabilities support security investigations involving misuse of corporate information assets. For these reasons, organizations typically reserve the right to monitor, log, and review all activities and messages that make use of their Internet resources.

2.4.6 Privacy Expectations

Because many organizations reserve the right to monitor, log, and review the activities on their Internet resources, users should have no expectation of privacy when using these resources to access, download, or transmit information. Moreover, the Internet Acceptable Use Standard should specifically state that users should have no expectations of privacy when using the organization's Internet resources.

2.4.7 Misuse Reporting

From time to time, users unwillingly receive communications from the Internet that contain objectionable content. In other cases, users are aware of others that are improperly using the organization's Internet resources. In either case, the Internet Acceptable Use Standard should require users to report misuse of Internet resources in a timely manner to designated contacts (for example, supervisors, department heads, Human Resources department, etc.).

2.5 Responsibilities

The Internet Acceptable Use 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 *Acceptable Use 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.

Table 1: Responsibilities and Assignments

Responsibilities	**Typically Assigned to**
Approves the standard.	Chief Information Security Officer (CISO)
Ensure the development, implementation, and maintenance of the standard.	Chief Information Security Officer (CISO) or Information Security Team.
• Ensure that the Internet Acceptable Use Standard is properly communicated and understood within respective organizational units. • Define, approve, and implement procedures in organizational units that are consistent with the Internet Acceptable Use Standard.	Management
• Comply with the Internet Acceptable Use Standard. • Report misuse of Company Internet Resources. • Cooperate with official Company security investigations.	Users

2.6 Enforcement and Exception Handling

The Internet Acceptable Use Standard should reiterate or expound upon the enforcement statement established in the *Acceptable Use 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 Internet Acceptable Use Standard should reiterate or expound upon the review and revision statements established in the *Acceptable Use Policy*.

3 Sample Internet Acceptable Use Standard

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

Sample Internet Acceptable Use Standard

The Company ABC (the "Company) *Acceptable Use Policy* defines objectives for establishing specific standards on the appropriate business use of information assets.

This *Internet Acceptable Use Standard* builds on the objectives established in the *Acceptable Use Policy*, and provides specific instructions and requirements on the proper and appropriate business use of Internet resources.

I. Scope

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

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

Internet Resources refer to the Company systems, networks, equipment, software, and processes that provide access to and/or use of the Internet, including accessing, downloading, transmitting, or storing data and information, as well as the operation of software products and tools.

Objectionable refers to anything that could be reasonably considered to be obscene, indecent, harassing, offensive, or any other uses that would reflect adversely on the Company including but not limited to comments or images that would offend, harass, or threaten someone on the basis of his or her race, color, religion, national origin, gender, sexual preference, or political beliefs.

Users refer to all individuals, groups, or organizations authorized by the Company to use Company Internet Resources.

II. Requirements

The requirements of the *Internet Acceptable Use Standard*, although specific, should not be considered a comprehensive listing. The Company considers consistency with requirements as the basis for considering the appropriateness of other activities and practices that are not specifically addressed.

A. Business Use

1. Company Internet Resources are provided primarily for official and authorized Company business use and purposes.

2. Limited personal use of Company Internet Resources is acceptable as long as it does not conflict with Company business and interests.

3. The use of Company Internet Resources shall be in accordance with applicable laws and regulations.

4. Users shall be accountable for all Internet activity associated with their accounts.

B. Improper Use

1. Any use of Company Internet Resources must not be illegal, must not be perceived as a conflict of Company interest, and must not interfere with normal business activities and operations.

2. Users shall not violate any laws or regulations through the use of Company Internet Resources.

3. Company Internet Resources shall not be used to link, bookmark, access, download, transmit, or store objectionable material, images, or content.

4. Company Internet Resources shall not be used to conduct personal or non-Company solicitations.

5. Participation in any chat groups, electronic bulletin boards, or forums is permitted only when conducting official and authorized Company business. Personal use of Company Internet Resources to participate in any chat groups, electronic bulletin boards, or forums is prohibited.

6. Users must not allow others to access the Internet by using their accounts.

C. Browser Software

1. Users can use only Company-approved versions and configurations of browser software when using Company Internet Resources.

2. Users must not adjust the browser security settings to be less restrictive than the Company-approved configuration.

D. Downloaded Materials

1. Company Internet Resources shall not be used to access, download, transmit, or operate any commercial software, shareware, or freeware that has not been authorized by the Company.

2. All material and content that has been downloaded using Company Internet Resources must be reviewed for malicious code and viruses in accordance with the *Asset Protection Policy* and the *Anti-Virus Standard*.

E. Right to Monitor

1. The Company reserves the right to monitor and review all activities and messages using Company Internet Resources.

2. The Company reserves the right to disclose the nature and content of any User's activities involving Company Internet Resources to law enforcement officials or other third parties without any prior notice to the User.

F. Privacy Expectations

1. Users should have no expectations of privacy when using Company Internet Resources.

G. Misuse Reporting

1. Actual or suspected misuse of Company Internet Resources should be reported in a timely manner to <Specify Contact>.

2. Upon the receipt or continued receipt of objectionable content, Users should contact <Specify Contact>.

III. Responsibilities

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

Company management is responsible for ensuring that the *Internet Acceptable Use Standard* is properly communicated and understood within their respective organizational units. Company management also is responsible for defining, approving, and implementing procedures in its organizational units and ensuring their consistency with the *Internet Acceptable Use Standard*.

Users are responsible for familiarizing themselves and complying with the *Internet Acceptable Use Standard* and the associated procedures provided by Company management. Individuals also are responsible for reporting misuse of Company Internet Resources and cooperating with official Company security investigations relating to misuse of such resources.

IV. Enforcement and Exception Handling

Failure to comply with the *Internet Acceptable Use 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 *Internet Acceptable Use 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 *Internet Acceptable Use Standard.*

V. Review and Revision

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

Approved: ____

Signature
<Insert Name>
Chief Information Security Officer