Developmental Electronic Mail Acceptable Usage Standard

By Michael D. Peters
March 2007

Warning and Disclaimer

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, Lazarus Alliance (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.

Introduction

This research report from Lazarus Alliance, Developmental Electronic Mail Acceptable Usage Standard, provides best practices guidance that organizations can reference and leverage to assess, improve, or develop an Electronic Mail Acceptable Usage Standard. The Electronic Mail Acceptable Usage Standard should provide specific instructions and requirements on the proper and appropriate business use of electronic mail resources. The insights provided in this report are derived from the considerable "real world" experience gained by Lazarus Alliance in developing and assessing Information Security policies, standards, guidelines, and procedures.

1. Audience

There are two primary audiences for this report:

1. Organizations that have implemented or are planning to implement the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Framework (HORSE).

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 Electronic Mail Acceptable Usage Standard, and to enhance communication of an overall Policy Framework.

This report assumes a certain level of understanding of the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Framework (HORSE) and terminology. This paper provides a high-level overview of the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Policy Framework (HORSE). Refer to the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Framework (HORSE) research report for more detailed and comprehensive information.

2. Background and Context

As shown in **Figure 1**, the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Policy Framework (HORSE) (The Policy 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.

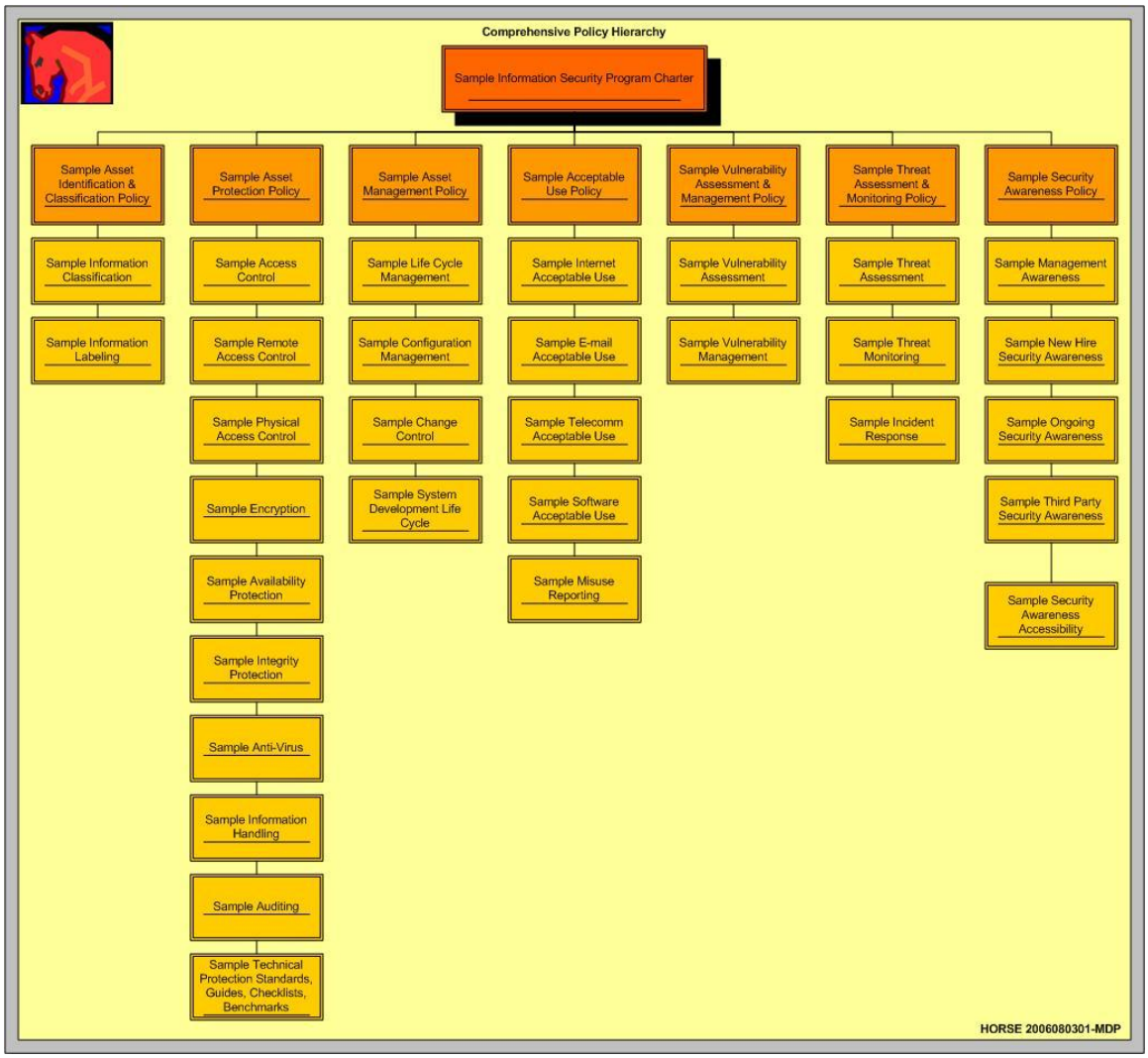

Figure 1: The Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Policy Framework (HORSE).

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 level.

Lazarus Alliance 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 Electronic Mail Acceptable Usage Standard that is traceable and consistent with the Framework.

3. Document Organization

The Key Considerations section discusses specific factors that organizations should consider when developing the Electronic Mail Acceptable Usage Standard.

The Sample Electronic Mail Acceptable Usage Standard section outlines a sample standard established on the basis of the key considerations discussed in the report.

Key Considerations

Lazarus Alliance 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 3 discuss key considerations for each major section of the Electronic Mail Acceptable Usage Standard.

Purpose Statement

As defined in the Lazarus Alliance sponsored Holistic Operational Readiness Security Evaluation Framework (HORSE), 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 Electronic Mail Acceptable Usage Standard should derive from the Acceptable Usage Policy (see **Figure 1**).

The Acceptable Usage Policy defines the objectives for establishing specific standards on the appropriate business use of information assets. The Electronic Mail Acceptable Usage Standard builds on these policy objectives by providing specific instructions and requirements on the proper and appropriate business use of electronic mail resources.

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 Electronic Mail Acceptable Usage Standard should reiterate the scope statement from the Acceptable Usage Policy.

Terms and Definitions

The Electronic Mail Acceptable Usage 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.
>
> **Electronic Mail Resources** – Should provide a definition that refers to the systems, networks, equipment, and software that provide access to and or use of electronic mail.
>
> **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 electronic mail resources.

Requirements

The Electronic Mail Acceptable Usage Standard should provide specific instructions and requirements on the proper and appropriate business use of electronic mail resources. However, it is not possible to develop or list specific requirements for every manner in which electronic mail resources may be used. The requirements of the *Electronic Mail Acceptable Usage 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, software and downloaded materials, as well as monitoring rights, privacy expectations, and storage capability.

Business Use

Electronic mail can provide significant business benefit for an organization. However, there may also be significant legal, security, and productivity issues related to how electronic mail resources are used. Stating that electronic mail resources are provided only for business use is both impractical and unenforceable. Business use issues typically are addressed by stating that the electronic mail resources are provided primarily for business purposes, and to support the organization's business goals. The business use requirements should provide details into the organization's business goals either through direct statements or referrals to other documents. Outlining these business goals will further establish the proper context for what actions are considered business use.

In addition, the business use requirements should state specific conditions for limited personal use of electronic mail resources. Personal use is typically considered acceptable as long as it does not conflict with business and corporate interests such as productivity, confidentiality, and reputation.

Because electronic mail is considered a corporate information asset, it should be protected accordingly. All outgoing electronic mail messages should include the organization's standard disclaimer statement that describes the proper use for the electronic mail message and its intended audience.

Improper Use

Although organizations may provide electronic mail 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 Electronic Mail Acceptable Usage Standard should prohibit the use of electronic mail resources for activities that are illegal, may have a negative impact on the organization's reputation, violate corporate policies, conflict with business interests, or interfere with productivity and business operations.

As previously stated, electronic mail resources should be used to support the organization's business goals. Electronic mail resources should not support any business endeavor, private or public, that is not directly related to the organization's business goals. Moreover, the use of electronic mail resources for personal profit should be prohibited.

Electronic Mail Software

Because the type of electronic mail software and its configuration can directly expose an organization's information assets, most organization will provide users with a standard electronic mail software package. The electronic mail software requirements for the Electronic Mail Acceptable Usage Standard should restrict users to approved and authorized software and configurations. The requirements also should list the approved electronic mail software packages and prohibit users from changing software configurations to less restrictive security settings. In addition, many electronic mail software packages support tasks such as automated message forwarding and anonymous senders. These tasks can pose significant risks and their use should not be allowed.

Downloaded Materials

Access to electronic mail allows users to attach programs, documents, and other materials to their messages, or to download materials. The contents and attachments of electronic mail messages can exploit existing vulnerabilities or introduce malicious code, viruses, or worms to the organization's information systems and networks. The downloaded materials requirements for the Electronic Mail Acceptable Usage Standard should prohibit users from downloading unauthorized software and documents, and restrict the types and sizes of attachments. They also should require downloaded materials to be reviewed for malicious code in accordance with established policies and standards. In addition, the requirements should discuss how electronic mail content and attachments are examined for violations, viruses, and worms.

Right to Monitor

Electronic mail can potentially introduce viruses and malicious code to an organization's information systems and networks. Therefore, many organizations use security controls and capabilities to monitor and examine the contents and attachments of electronic mail messages, as well as to support security investigations involving misuse of corporate information assets. The right to monitor requirements should state why and how the organization monitors electronic mail messages.

Privacy Expectations

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

Storage Capacity

Most companies perform routine backups to support data recovery efforts for production systems. Messages stored on electronic mail servers are usually included as part of the backup procedure. Unlimited storage of electronic mail messages may not only adversely impact system performance and the duration of the routine backups but also may expose electronic mail servers to attacks that attempt to fill up file systems. The storage capacity requirements should encourage users to delete messages in a timely manner and specify the approved retention time for electronic mail messages stored locally or on a server.

Responsibilities

The Electronic Mail Acceptable Usage 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 Usage 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 Electronic Mail Acceptable Usage Standard is properly communicated and understood within respective organizational units. Define, approve, and implement procedures in organizational units that are consistent with the Electronic Mail Acceptable Usage Standard.	Management
Comply with the Electronic Mail Acceptable Usage Standard. Report misuse of Company Electronic Mail Resources. Cooperate with official Company security investigations.	Users

Enforcement and Exception Handling

The Electronic Mail Acceptable Usage Standard should reiterate or expound upon the enforcement statement established in the Acceptable Usage 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.

Review and Revision Expectations

The *Electronic Mail Acceptable Usage Standard* should reiterate or expound upon the review and revision statements established in the Acceptable Usage Policy.

Sample Electronic Mail Acceptable Usage Standard

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

Sample Electronic Mail Acceptable Use Standard

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

This Electronic Mail Acceptable Use Standard builds on the objectives established in the Sample Acceptable Use Policy, and provides specific instructions and requirements on the proper and appropriate business use of Electronic Mail 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 and use of Company Electronic Mail Resources, are covered by this standard and must comply with associated guidelines and procedures.

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

Electronic Mail Resources refer to the Company systems, networks, equipment, software, and processes that provide access to and/or use of the electronic mail, 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 access and use Company Electronic Mail Resources.

II. Requirements

1. Business Use

i. Company Electronic Mail Resources are provided primarily for official and authorized Company business use and purposes in support of the following business goals and objectives:

<List, reference, or describe business goals>

ii. Limited personal use of Company Electronic Mail Resources is acceptable as long as it does not interfere with normal business operations, conflict with business interests, or has an adverse impact on the reputation of the Company.

iii. The use of Company Electronic Mail Resources shall be in accordance with applicable laws and regulations.

iv. Users shall be accountable for all Electronic Mail activity associated with their accounts.

v. All electronic mail transmissions outside the Company must have the following disclaimer attached:
   a. "This E-mail and any of its attachments may contain <**Company**> proprietary information, which is privileged, confidential, or subject to copyright belonging to the <**Company**>. This E-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this E-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this E-mail is strictly prohibited and may be unlawful. If you have received this E-mail in error,

please notify the sender immediately and permanently delete the original and any copy of this E-mail and any printout."

2. Improper Use

i. Any use of Company Electronic Mail Resources must not be illegal, must not constitute or be perceived as a conflict of Company interest, must not violate Company policies, and must not interfere with normal business activities and operations.

ii. Users shall not violate any laws or regulations through the use of Company Electronic Mail Resources.

iii. Company Electronic Mail Resources shall not be used to forward chain letters, virus warnings, and hoaxes or support other such "re-mailing" activities.

iv. Company Electronic Mail Resources shall not be used to download, transmit, or store objectionable material, images, or content.

v. Company Electronic Mail Resources shall not be used to conduct personal or non-Company solicitations.

vi. Users must not allow others to access Electronic Mail Resources by using their accounts.

vii. Company e-mail systems are intended for authorized business purposes.

viii. All messages sent over Company communications systems are the property of the company.

ix. To properly maintain and manage this property, management reserves the right to examine all data stored in, or transmitted by, these systems.

x. Communications must not be sent in any manner that could reasonably cause distress, embarrassment, or unwarranted attention, as this may constitute harassment. There will be no personal attacks, including any based on race, color, religion, sex, sexual orientation, national origin, age, disability, veteran status, or any other factors prohibited by law.

xi. The retrieval or distribution of chain letters or copyrighted

material is not permitted.

xii. E-mail communications may not be made anonymously and must be made by authenticated users.

xiii. Impersonation, misrepresentation, or unauthorized disclosures are not permitted.

xiv. Advertising or listings for personal benefit may not be generated.

3. Electronic Mail Software

i. Only Company approved versions and configurations of electronic mail software may be used. The following electronic mail software is authorized for use:

<Insert list of software>

ii. Users must not adjust the electronic mail software security settings to be less restrictive than the Company-approved configuration.

iii. Users shall not use software or features that automatically forward electronic mail messages.

iv. Users shall not use software or features (such as an anonymous mail sender) that obscures or masks the identity of the message sender.

4. Downloaded Materials

i. Company Electronic Mail Resources shall not be used to send, receive or store any commercial software, shareware, or freeware without the Company's prior written authorization.

ii. The content and attachments of electronic mail messages must be reviewed for malicious code and viruses in accordance with the Sample Asset Protection Policy and the Sample Anti-Virus Standard.

iii. For security and performance purposes, electronic mail attachments must be less than <**Enter size limit**>.

5. Right to Monitor

i. All Electronic Mail Resources and all messages created, received, processed, transmitted, and or stored on Company Electronic Mail Resources are Company information assets and property.

ii. The Company reserves the right to monitor and review all activities and messages using Company Electronic Mail Resources at any time by authorized Company personnel.

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

6. Privacy Expectations

i. Users should have no expectations of privacy when using Company Electronic Mail Resources.

7. Storage Capacity

i. Users shall delete unnecessary electronic mail message to avoid unnecessary accumulation of storage on the Company electronic mail servers.

ii. Electronic mail messages containing business critical information should be stored on production servers to ensure proper data backup.

iii. The approved record retention period for electronic mail messages is <**Insert number**> days.

8. Misuse Reporting

i. Actual or suspected misuse of Company Electronic Mail Resources should be reported in accordance with the Misuse Reporting Standard.

ii. Upon the receipt or continued receipt of objectionable electronic mail, Users should contact **<Specify Contact>** in accordance with the *Sample Misuse Reporting Standard*.

III. Responsibilities

The Chief Information Security Officer (CISO) approves the *Electronic Mail Acceptable Use Standard*. The CISO also is responsible for ensuring the

development, implementation, and maintenance of the *Electronic Mail Acceptable Use Standard*.

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

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

IV. Enforcement and Exception Handling

Failure to comply with the *Electronic Mail 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 *Electronic Mail 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 *Electronic Mail Acceptable Use Standard*.

V. Review and Revision

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

Approved: _____

Signature
<Insert Name>
Chief Information Security Officer