Anti-Malware Standard

Global Eagle™ Information Security Standard

Revision 1.0

8/7/2018

Effective date (update for each revision)	Document Owner	Document ID
8/7/2018	Igor Spektor	900.03

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Anti Malware Standard should be retained in hard copy format in case Global Eagle Entertainment online systems are unavailable during an Incident

1 Table of Contents

2 Copyright, Trademarks, Notice of Proprietary Rights

2.1 COPYRIGHT

Information in this document may change without notice and does not represent a commitment on the part of Global Eagle™.

Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice. The claim of copyright does not imply waiver of Global Eagle's other rights. See notice of Proprietary Rights.

2.2 TRADEMARKS

The Global Eagle™ logos are registered trademarks of Global Eagle™.

All other company and product names used herein may be the trademarks or registered trademarks of their respective companies.

2.3 NOTICE OF PROPRIETARY RIGHTS

This documentation is a confidential trade secret and the property of Global Eagle™ and contains Global Eagle's Confidential, Proprietary, or Privileged Information. Use, examination, reproduction, copy, de-compilation, transfer, and disclosure to others are strictly prohibited except by express written agreement with Global Eagle™.

3 Revision History

Date	Version	Prepared By	Document Changes
5/4/2018	Initial Draft	Stephen Mitchell	Initial Draft
8/7/2018	Revision 1.0	Stephen Mitchell	Revision 1.0

Table 1: Revision History

4 Approvals

Name	Title	Reviewed By	Approved By	Date
Igor Spektor	Head of Information Security and Compliance	Igor Spektor		8/7/2018

Table 2: Approvals

5 Points of Contact

Name	Title	Email	Contact Number
Igor Spektor	VP, Head of Information Security and Compliance	Igor.Spektor@globaleage.com	+1-954-401-9155

Table 3: Points of Contact

6 Associated References

Associated Standard Numbers	Associated Procedure Numbers	Associated Policy Numbers
900.01 - Information Classification and Safeguards Standard	900.00.01 - Security Policy Exception Form	900 - Information Security Policy

Table 4: Associated References

7 Introduction

7.1 Audience

This document is intended for use by Global Eagle™ and its subsidiaries (Global Eagle)'s management, employees, external auditors, risk advisors, outside labor and service providers, globally.

7.2 Assumptions

This document is annually reviewed and updated, to reflect changes to Global Eagle's business processes and IT environments.

7.3 Owner and Contact

Global Eagle's Chief Information Security Officer is the single point of contact for questions about this document.

7.4 Distribution

This is an electronically controlled and issued document. The latest electronic version of the document is available at the Global Eagle™ Information Technology page here. Users should always confirm they are using the latest electronic version of the document.

8 Scope and Purpose

This standard provides guidance on protecting the integrity of software and information from malicious code (a.k.a. Malware).

Malicious code is any program that acts in an unexpected and potentially damaging manner. Common types of malicious code include:

TRAPDOOR: An entry point into a program that is usually bypassed during the development process. Usually, these entry points would be closed when the program development is completed. However, they can be left open either intentionally or unintentionally.

LOGIC BOMB: A program that triggers an unauthorized, malicious act when some pre-defined condition occurs.

WORM: A worm is a program that tunnels through a network by gaining access privileges. Worms can tie up all the computing resources on a network and essentially shut it down.

TROJAN HORSE: A program that appears to function as anticipated but that contains additional, hidden functions that allow unauthorized collection, falsification, or destruction of data. The Trojan horse is the most commonly used method for program-based frauds and sabotage and for disguising viruses.

VIRUS: A typical virus is a small computer program that, as part of its operations, reproduces itself by making copies of itself and inserting these copies into uninfected programs or data files. This insertion process takes only a fraction of a second, a virtually undetectable delay. The infected program will subsequently execute the virus code during its normal processing. In addition to its ability to reproduce, the virus may cause damage to the programs, data, or equipment, or it may perform some other function that is relatively harmless.

9 Anti-Malware Standard

9.1 Anti-Virus Software

Inbound, internally transported or outbound data, except for active content that is assessed to be susceptible to malicious code must be scanned before storage, execution or distribution. After storage, data that are assessed to be susceptible to malicious code must be scanned regularly.

9.1.1 Requirements

9.1.1.1 Use of Virus Detection Software

All Global Eagle™ servers, workstations, and laptop computers should have approved virus detection or integrity software installed and active. This software should be configured to continuously monitor the systems and files for characteristics of viruses, worms, spyware, and Trojan Horses should be capable of generating audit logs and should be installed in "auto-protect," "full-time" or "real-time" mode.

9.1.1.2 Virus Detection Software Configuration

Virus detection software should be configured as follows:

- At system startup, the software should perform a scan of the system that includes, but is not limited to, the Master Boot Record, any other local boot records, and also perform an integrity check of the anti-virus software itself. (Typically this is included in the software's default settings.)
- The software should clean infected files automatically. If a repair is not possible, the software should deny access to the infected file.
- The memory resident portion of the software should be loaded and enabled at system startup and:
    - Scan all files when opened, copied, moved, created or downloaded.
    - Check removable media for boot viruses upon access and when rebooting the computer.
    - Non-administrative end users should not be able to disable, change the settings or circumvent the anti-virus software.

- The software should, when an infected file is found and repaired:
    - Sound an audible alert and display an alert message.
    - Forward an alert message to Anti-Virus Support and/or to a local administration server for analysis.
- When possible, end users should be prevented from disabling or unloading the virus detecting software.

9.1.1.3 Updating Anti-Malware Software

Since signature-based anti-virus, spam, and spyware protection products scan for unique components of certain known malicious code, they should be updated continually. These signatures should be updated at least once a day to ensure systems scans can identify all known viruses. When possible, updates should be installed as part of an automated network process (e.g., via login scripting).

9.1.1.4 Scheduling Virus Scans

Whenever possible, virus scans should be scheduled to occur automatically following the schedule as identified in the "Scanning Frequency" requirement.

9.1.1.5 Scanning Frequency

Virus scans of permanent media should be performed at least daily on:

- All servers connected to the Global Eagle's network, including all third-party servers connected to the Global Eagle's network.
- All computers used for the distribution of files to third parties.
- Any workstation that shares software with any other computer.
- All computers are running an application for which the loss of data or loss of the application poses a risk of embarrassment or monetary loss to Global Eagle™ .

For all situations not covered above, virus scanning should be performed at least weekly.

9.1.1.6 Scanning Electronic Mail

Electronic mail transmitted from Global Eagle™ or received via the Internet should be scanned for viruses, worms, and Trojan Horses at the mail server, prior to being transmitted or delivered to its intended recipient.

9.1.1.7 SPAM Protection

The Global Eagle's email system should provide SPAM protection.

9.1.1.8 Virus Detection of Inbound Files

Virus scans or integrity checks should be completed before the first use of each executable file that is brought into the Global Eagle's computing environment. This includes, but is not limited to:

- Program files copied from vendor sites (i.e., trusted or untrusted).
- Updates to program files copied from a vendor site.
- All files copied from Websites.

This should be accomplished by installing approved anti-virus software on all Global Eagle™ Internet gateways that permit inbound connections.

9.1.1.9 Scanning Outbound Files

All outbound files should be scanned at the mail server, prior to leaving the Global Eagle's network to ensure Global Eagle™ is not forwarding any viruses, worms or Trojan Horses to partners, clients or vendors.

9.1.1.10Scanning Removable Media

Virus scans or integrity checks should be performed before any removable media being sent outside the Global Eagle™ . It is the responsibility of the user sending the removable media outside Global Eagle™ to perform the necessary virus scans using Global Eagle™ approved anti-virus software.

Also, virus scans or integrity checks should be performed on all removable media received prior to the files being read.

9.1.1.11 Audit Logs of Scan Results

It is advised to follow this approach across the board for all systems; however, for PCI (Payment Card Industry) relevant systems; audit logs of scan results should be kept for at least for three (3) months in the online system and at least one (1) year archived offline. These logs should note the date and times that scans occurred and any findings that were identified.

9.2 Responsibilities, Training, and Actions

Information Security and Information Technology are responsible for developing, implementing, maintaining and communicating a malicious code control program.

Formal procedures should be documented and communicated to help desk and support personnel informing them of their responsibilities when malicious code-related activity is reported.

The installation of software on Global Eagle™ -owned or -leased information resources by unauthorized personnel is prohibited, unless prior written management approval has been given.

Global Eagle™ personnel, third-party consultants, contractors, and vendors should not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of, or access to, any Global Eagle™ information resource.

Information Security is responsible for immediately notifying any Global Eagle™ personnel and third parties who could be affected by an intrusion or malicious code activity. If communication to a third party is required, Legal & Compliance and Corporate Communications should review and authorize the communication.

9.2.1 Requirements

9.2.1.1 Responsibilities for Malicious Code Program

Information Security and Information Technology are responsible for developing, implementing, maintaining and communicating a malicious code control program to limit the introduction and spread of computer viruses, worms, Trojan Horses, spam, spyware, denial of service attacks, etc., within the Global Eagle's computing environments. They are also responsible for reviewing and selecting approved virus detection software to be used by Global Eagle™ .

9.2.1.2 Introduction of Malicious Code

The installation of software on Global Eagle™ -owned or -leased information resources by unauthorized personnel is prohibited, unless prior written management approval has been given.

Global Eagle™ personnel, third-party consultants, contractors, and vendors should not intentionally write, generate, compile, copy, collect, propagate, execute or attempt to introduce any computer code designed to self-replicate, damage or otherwise hinder the performance of, or access to, any Global Eagle™ information resource. If such activity is verified, it is grounds for immediate termination.

Where the use of mobile code is authorized, the configuration should ensure that the authorized mobile code operates according to a clearly defined security policy, and unauthorized mobile code should be prevented from executing.

9.2.1.3 Virus Infections

If any Global Eagle™ employee, contractor or service provider detects a virus on permanent or removable media, the following procedures should be followed:

- Attempt to repair the virus with Global Eagle™ -approved anti-virus software.
- If the virus cannot be repaired, isolate the affected computer immediately by disconnecting it from the network.
- Isolate all diskettes or other media that have been recently used on that computer. Do not allow these media to be mounted on other computers or network servers until they have been evaluated for possible infection, and if appropriate, cleaned.
- Contact the appropriate technical support staff (e.g., LAN system administrator) at your location or the Help Desk for assistance in virus diagnosis and treatment.
- Contact Information Security to record the virus incident if:
    - External customers or third parties are involved.
    - The infected document or file was widely distributed.
    - The virus cannot be repaired.
    - The virus poses a serious threat to any Global Eagle™ information resource.

9.2.1.4 Escalation Procedures

Formal procedures should be documented and communicated to help desk and support personnel informing them of their responsibilities when malicious code-related activity is reported. It is the responsibility of Information Security to ensure that help desk and support personnel are adequately trained. Also, escalation procedures should be documented to ensure that notification of virus activity is sufficient to minimize virus spread.

Information Security is responsible for immediately notifying any Global Eagle™ personnel and third parties who could be affected by an intrusion or malicious code activity. If communication to a third party is required, Legal & Compliance and Corporate Communications should review and authorize the communication.

9.2.1.5 Training Global Eagle™ Personnel on the Use of Virus Detection Software

Global Eagle™ personnel should be trained on the proper procedures for using virus detection software and responding to a virus, worm, Trojan Horse, etc. This training information should be included in the overall training and awareness program that is the responsibility of Information Security.

10 Standard Exceptions

All standard exceptions must be approved by the Chief Information Security Officer.

11 Standard Violation

Violations of the standards in this document may subject involved employees to corrective action up to and including termination of employment.

12 Table of Tables