

# Web Services Security Standard

Global Eagle Information Security Standard

Revision 1.0

8/10/2018

| Effective date ( <i>update for each revision</i> ) | Document Owner | Document ID |
|----------------------------------------------------|----------------|-------------|
| 8/10/2018                                          | Igor Spektor   | 900.15      |



6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

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

# 1 Table of Contents

---

|     |                                                           |                                     |
|-----|-----------------------------------------------------------|-------------------------------------|
| 1   | Table of Contents .....                                   | 2                                   |
| 2   | Copyright, Trademarks, Notice of Proprietary Rights ..... | 3                                   |
| 2.1 | COPYRIGHT .....                                           | 3                                   |
| 2.2 | TRADEMARKS .....                                          | 3                                   |
| 2.3 | NOTICE OF PROPRIETARY RIGHTS .....                        | 3                                   |
| 3   | Revision History .....                                    | 4                                   |
| 4   | Approvals .....                                           | 4                                   |
| 5   | Points of Contact .....                                   | 4                                   |
| 6   | Associated References .....                               | 5                                   |
| 7   | Introduction .....                                        | 6                                   |
| 7.1 | Audience .....                                            | 6                                   |
| 7.2 | Assumptions .....                                         | 6                                   |
| 7.3 | Owner and Contact .....                                   | 6                                   |
| 7.4 | Distribution .....                                        | 6                                   |
| 8   | Scope and Purpose .....                                   | 7                                   |
| 9   | Access Management Standard .....                          | <b>Error! Bookmark not defined.</b> |
| 10  | Standard Exceptions .....                                 | 12                                  |
| 11  | Standard Violation .....                                  | 12                                  |
| 12  | Table of Tables .....                                     | 13                                  |



## 2 Copyright, Trademarks, Notice of Proprietary Rights

---

### 2.1 COPYRIGHT

2018 by Global Eagle™. All rights reserved.

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 |
|-----------|---------------|------------------|------------------|
| 5/29/2018 | Initial Draft | Stephen Mitchell | Initial Draft    |
| 8/10/2018 | 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 |             | 8/10/2018 |

*Table 2: Approvals*

### 5 Points of Contact

| Name         | Title                                           | Email                                                                        | Contact Number  |
|--------------|-------------------------------------------------|------------------------------------------------------------------------------|-----------------|
| Igor Spektor | VP, Head of Information Security and Compliance | <a href="mailto:Igor.Spektor@globaleage.com">Igor.Spektor@globaleage.com</a> | +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.



## 7.5 Scope and Purpose

This standard establishes requirements for information release on Global Eagle owned publicly available websites and services.

The integrity of electronic information that is published on a publicly available system (e.g., publishing information on a Web server) that is accessible via the Internet must be reliably safeguarded against unauthorized changes. Formal prior authorization must be obtained for the publication of any information on publicly available information systems. The authorization procedure must ensure that such information does not violate any laws.

Software, data, and other information for which a high degree of integrity is required and that is published on a publicly available system, are to be provided with suitable security safeguards, e.g., encryption techniques such as Secure Socket Layers (SSL) on Web servers.

Due to its nature, the web infrastructure is permanently connected to the internet. This could result in attacks specifically targeted to these infrastructures by anyone who has internet access. Therefore, not only the applicable requirements from the other Global Eagle security policies and standards, but also the additional requirements specified in this standard, must be met.



## 8 Web Services Security Standard

---

### 8.1 Robust Web Infrastructure

This standard provides guidance for a robust web infrastructure for hosting publicly available website/service.

#### 8.1.1 Requirements

The web infrastructure used to deliver information and transaction services via the internet to customers or the general public must be robust and resistant to attacks to ensure the integrity, confidentiality and availability of information and services delivered via this web infrastructure.

- All browser-based access from the internet to Global Eagle's web infrastructure must only be possible through public facing web servers.
- The data processing applications must be implemented on application servers that are isolated (logically separated, for example by operating system compartments or restricted network segments) from the public facing web servers. Requests for application functions must be forwarded by the public facing web servers to the application servers. Application servers must be connected to public facing web servers only via authenticated connections.
- Code sent to the web user (for example HTML, scripts) must not include descriptive information that can be used to attack the system (for example directory structure, database names, network IDs, software version, and programmer's name).
- All input data that could influence systems behavior (including URL requests, SQL injections, HTTP headers) must be properly validated on the server before processing (for example URL requests by a web page navigator) to prevent unauthorized access, buffer overflow, undesirable page navigation or other unwanted behavior.
- Access to directories and files must be secured by proper authorization settings that provide only the minimal access required for correct operation.
- Error messages presented to web users must only contain information that is relevant to the user (for example it must not disclose code segments or details of the web infrastructure and its operation).
- Security events in the web infrastructure must be logged and monitored.
- Web sessions with controlled access must be locked or terminated after session inactivity of maximum 15 minutes.



- Confidential web content, such as passwords and private client information, must not remain cached within the web infrastructure after session termination.
- Depending on the criticality of the services a real-time alerting mechanism must be in place to ensure that immediate action is taken in the event of (temporary) site unavailability or disruption of services.

In situations where visitors of Global Eagle websites can exchange Confidential/Secret information during a web session with Global Eagle, the web infrastructure must offer the possibility to verify the authenticity of the web server (e.g. SSL certificate verified by a recognized public Certificate Authority) and must enable a secure browser-to-server connection.

## 8.2 Reliability of Web Content

This standard establishes requirements for authorizing information for release on publicly available systems.

### 8.2.1 Requirements

Users of web pages must be informed of the level of reliability of all web content that Global Eagle presents.

For all Global Eagle information published on publicly available systems (e.g., the worldwide Web), an author should be designated.

Content approvers should be assigned by the head of a business unit.

Authors should have publishing responsibility and necessary training, which is recognized by their line manager/supervisor and should be sponsored by an approver.

All content published on Global Eagle web sites must have a nominated owner. Procedures for content management must be in place; related responsibilities must be clearly assigned by the owner.

Web sites must include a disclaimer that clearly specifies to users what value (for example, correctness, timeliness, completeness) can be attached to the web content presented on the site. The disclaimer must have Legal approval. To ensure that users are aware of the disclaimer and have easy access to it, the disclaimer must be published at least on the website home page and when feasible on other frequently visited web pages. The disclaimer must also cover third-party web content included in Global Eagle internet pages.



#### Note



It is good practice to have a contact e-mail address on the home page of any website to enable visitors of the website to send in comments with regard to incorrect or inconsistent web content published on the site. When doing so, feedback and prompt follow-up to individuals that send in comments are important to maintain public confidence.

### 8.2.1.1 Web Content Approvers

Content approvers should be assigned by the Global or Regional head of a business unit, have the authority and desire to take responsibility of the published content, and have the appropriate level of knowledge regarding legal responsibilities and risks of publishing public information. Approvers are responsible for:

- Ensuring the published content is classified for public consumption
- Reviewing content for accuracy
- Ensuring appropriate personnel have reviewed and signed off on the content
- Ensuring the content displayed follows Global Eagle's policies and standards

Content approvers cannot self-approve documents they have authored.

### 8.2.1.2 Web Content Authors

Authors should have publishing responsibility and necessary training, which is recognized by their line manager/supervisor and should be sponsored by an approver. Authors are responsible for ensuring that the content:

- Is correctly classified for public consumption
- Complies with applicable laws and regulations
- Complies with Global Eagle's style and layout guidelines

## 8.3 Privacy Statements

This standard establishes requirements for privacy statement on websites.

### 8.3.1 Requirements

Users of Global Eagle web pages must be informed of the way in which personal information is handled by Global Eagle.

Web sites must include or refer to a privacy statement that clearly specifies to users how user information obtained via the browser cookie mechanism or typed in by the user will be dealt with. The privacy statement must have Legal approval. To ensure that users are aware of the privacy statement and have easy access to it, the privacy statement must at least be published on the website home page and when feasible on other frequently visited web pages.

## 9 Standard Exceptions

---

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

## 10 Standard Violation

---

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



# 11 Table of Tables

Table 1: Revision History .....4

Table 2: Approvals.....4

Table 3: Points of Contact .....4

Table 4: Associated References .....5

