Application Development Security Standard

Global Eagle™ Information Security Standard

Revision 1.0

8/7/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
8/8/2018	Igor Spektor	900.04

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Application Development 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 5
2.1 COPYRIGHT 5
2.2 TRADEMARKS 5
2.3 NOTICE OF PROPRIETARY RIGHTS 5
3 Revision History 6
4 Approvals 6
5 Points of Contact 6
6 Associated References 7
7 Introduction 8
7.1 Audience 8
7.2 Assumptions 8
7.3 Owner and Contact 8
7.4 Distribution 8
8 Scope and Purpose 8
9 Application Development Security Standard 9
9.1 Application Development Methodology 9
9.1.1 Requirements 9
9.1.1.1 Definition of Interfaces 9
9.1.1.2 File Requirements Definition and Documentation 9
9.1.1.3 Input Requirements Definition and Documentation 9
9.1.1.4 Integrating Security Tasks into the Systems Development Life Cycle (SDLC) 10
9.2 Development Environment Security 10
9.2.1 Requirements 10
9.2.1.1 Isolation of Application Development Activities 10
9.2.1.2 Segregating Development and Production Duties 10
9.2.1.3 Protecting Source Code 11
9.2.1.4 Access to Program Source Libraries 11
9.3 Business Requirements 11

9.3.1 Requirements 11
9.3.1.1 Approval of Business Requirements 11
9.3.1.2 Information Security Review of Business Requirements 12
9.3.1.3 Integrating Security Requirements in System Design 12
9.4 Risk Assessment 12
9.4.1 Requirements 13
9.5 Security of Installation Process 13
9.5.1 Requirements 13
9.5.1.1 Implementation Plan 14
9.5.1.2 Production Installs Should Follow a Formal Process 14
9.5.1.3 User Procedures and Training 14
9.6 Software Acquisition 15
9.6.1 Requirements 15
9.6.1.1 Escrow of Source Code 15
9.6.1.2 Evaluating Software for Security Safeguards 15
9.6.1.3 Analysis of Packaged Software Security Risks 16
9.7 Application Testing 16
9.7.1 Requirements 16
9.7.1.1 Review of Application Security Features 16
9.7.1.2 Approving Production Software 16
9.7.1.3 Checks Prior to Promoting Applications to Production 17
9.7.1.4 Security Verification Tests 17
9.7.1.5 Approval for Using Production Data for Testing 18
9.8 Secure Design 18
9.8.1 Requirements 18
9.8.1.1 Application Controls 18
9.9 Application Security Controls 19
9.9.1 Requirements 19
9.9.1.1 Input Data Validation 20
9.9.1.2 Data Processing Controls 20
9.9.1.3 Use of Message Authentication Controls 20
9.9.1.4 Output Data Validation 21

9.9.1.5 Application Auditing / Logging 21
10 Standard Exceptions 22
11 Standard Violation 22
12 Table of Tables 23

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
8/8/2018	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		8/8/2018

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 designing, building and purchasing secure applications.

9 Application Development Security Standard

9.1 Application Development Methodology

This standard establishes requirements for ensuring that all internal application development activities adhere to accepted industry processes.

9.1.1 Requirements

All internal development efforts should follow Global Eagle's Systems Development Life Cycle methodology.

9.1.1.1 Definition of Interfaces

The system development life cycle methodology should provide that all external and internal interfaces are correctly specified, designed and documented.

9.1.1.2 File Requirements Definition and Documentation

The system development life cycle methodology should provide that an appropriate procedure is applied for defining and documenting the file format for each information system development or modification project. Such a procedure should ensure that the pre-defined data dictionary rules are respected.

9.1.1.3 Input Requirements Definition and Documentation

The organization's system development life cycle methodology should require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project.

9.1.1.4 Integrating Security Tasks into the Systems Development Life Cycle (SDLC)

Information Security should work with software engineering groups to integrate security tasks into Global Eagle's Systems Development Life Cycle methodology, ensuring that security considerations and procedures are integrated throughout the development lifecycle. Examples of topics to be covered include:

- Transactions should be conducted in a manner that makes them highly resistant to tampering throughout the entire process.
- Records should be stored, accessed and modified in a manner that makes them highly resistant to tampering.
- Transaction and recording keeping processes should be designed in a manner as to make it virtually impossible to circumvent detection of unauthorized changes.

9.2 Development Environment Security

This standard establishes requirements to ensure a secure environment is provided for development activities.

9.2.1 Requirements

Application documentation should be kept up to date, held in accessible form, and protected against loss or damage.

Application development/test activities such as program coding and software package customization should be isolated from production information resources.

Program source code should be protected.

Documentation of application development activity should be maintained, including development logs, approvals and project plans.

9.2.1.1 Isolation of Application Development Activities

Application development/test activities such as program coding and software package customization should be isolated from production information resources.

9.2.1.2 Segregating Development and Production Duties

Development and production maintenance duties should be assigned to separate personnel to ensure segregation of duties.

9.2.1.3 Protecting Source Code

Program source code should be protected by:

- Avoiding storage on production information resources.
- Restricting access to designated development personnel.
- Segregating source code under development from programs that are in production.
- Logging access.
- Periodically archiving older versions of code.

9.2.1.4 Access to Program Source Libraries

In order to reduce the potential for software corruption, access to program source libraries should be strictly maintained by applying the following principles:

- A program librarian should be nominated for each application.
- An audit log of all access to program source libraries should be maintained.
- Program listings should be held in a secure environment.
- Source control software should be used.

Program source libraries should exist for development, test and production.

9.3 Business Requirements

This standard establishes requirements for documenting business requirements before detailed design/specification begins and Security Integration within Business requirements.

9.3.1 Requirements

9.3.1.1 Approval of Business Requirements

Business requirements should be approved by the Information Owner, Information Security, Business Sponsor, and the Project Manager responsible for the development effort.

9.3.1.2 Information Security Review of Business Requirements

Information Security should review and approve security requirements for systems that will be used to process classified information before the initiation of project design. The review process should address requirements related to information security, internal controls, privacy protection and legal/regulatory considerations.

9.3.1.3 Integrating Security Requirements in System Design

To ensure that information security requirement is treated as an integral part of business requirements, security considerations should be integrated with design and specification efforts. Business requirements should be clearly defined in terms of scope, resources (i.e., including timing and costs), roles and responsibilities. They should be documented and supported by the requirements change process. The specification should take into account requirements for:

- System capacity, availability, continuity, flexibility, connectivity, and compatibility.
- Information processing, storage, and transmission, including requirements for protecting integrity and confidentiality.
- Arrangements needed to support the application in the production environment.
- Compliance with contractual, legal and regulatory obligations.
- Access control arrangements, such as access by particular types of users or from particular locations.
- Segregation of critical job duties or functions (e.g., ensure that no single individual could enter, authorize and complete a transaction).
- ·Segregating functions by the server (e.g., Web servers, database servers, and DNS should be implemented on separate servers.).

9.4 Risk Assessment

This standard establishes requirements for identifying key risks associated with applications under development and determining the controls required in order to keep those risks within acceptable limits.

9.4.1 Requirements

A risk assessment should be performed to determine the security risks of an application prior to implementation, integration, or purchase from a third party vendor following Global Eagle's Information Security Risk Assessment Process. Risk factors that should be considered include:

- The criticality of the application.
- The value, sensitivity of the information involved.
- The past experience of system infiltration or misuse.
- The extent of system interconnection.

The result of this risk assessment determines the security controls that should be engineered into the application. All outsourced software development efforts are subject to the same risk assessment process as internal development efforts.

9.5 Security of Installation Process

This standard establishes requirements for securely installing applications in a production environment.

9.5.1 Requirements

All default, pre-set, or temporary passwords and accounts assigned internally should be set to a unique value per user and changed immediately after first use.

Vendor-supplied defaults should be changed during installation of third party software on the network. This includes, but is not limited to the following:

- Passwords.
- Elimination of unnecessary accounts / user IDs (i.e. guest).
- Simple Network Management Protocol [SNMP] community strings.
- Encryption keys.
- Service Set Identifier (SSID).
- Disabling of SSID broadcasts.
- ·Enabling of Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.

9.5.1.1 Implementation Plan

An implementation plan should be prepared, reviewed and approved by relevant parties and be used to measure progress. The implementation plan should address site preparation, equipment acquisition, and installation, user training, installation of operating software changes, implementation of operating procedures and conversion.

9.5.1.2 Production Installs Should Follow a Formal Process

To ensure that applications are installed in the production environment on time and without disruption to information processing activities, installations in the production environment should be scheduled in advance and should follow formal change management and installation process. The installation process should include the following steps:

- Validating the load or conversion of data files.
- Restricting the installation of new or significantly-changed software.
- Implementing new/revised procedures, documentation and discontinuing older versions.
- Arranging for a rollback in the event of failure.
- Informing the individuals involved in their roles and responsibilities.
- ·Handing over responsibility to the individuals running the production environment.
- ·Logging installation activity.

9.5.1.3 User Procedures and Training

Prior to an application entering production, user training should be completed that includes training users on information security tasks and responsibilities. Users of significantly-changed applications should be involved in, or contribute to, the development processes and should be supported by documented procedures and help facilities.

9.6 Software Acquisition

This standard establishes requirements for the acquisition and use of third party software or applications.

9.6.1 Requirements

Global Eagle™ employees, third-party contractors, and vendors should adhere to all copyright laws and packaged software license agreements.

Unless made available as Commercial Off The Shelf (COTS) Software, a copy of the source code for all mission-critical applications developed by third parties should be provided to Global Eagle™ or placed in escrow with a third party escrow provider.

Prospective packaged software should be evaluated for the software's ability to provide adequate security safeguards.

Third-party software vendors should guarantee code integrity and the absence of backdoors.

Packaged software products should only be duplicated in accordance with license agreements (i.e., a backup copy for protection). The use of copy protection bypass software is prohibited for all employees. If problems do occur with master copies of software, the situation should be resolved directly with the vendor or authorized vendor representative.

9.6.1.1 Escrow of Source Code

Unless made available as Commercial Off The Shelf (COTS) Software, a copy of the source code for all mission-critical applications developed by third parties should be provided to Global Eagle™ or placed in escrow with a third party escrow provider. Business unit management should determine if the source code is mission critical and should consider the advice of Legal in making the determination.

Any changes to the source code over time should also be provided to Global Eagle™ or placed in escrow with a third party escrow provider.

9.6.1.2 Evaluating Software for Security Safeguards

Prospective packaged software should be evaluated for the software's ability to provide adequate security safeguards against unauthorized use or modification of data.

Third-party software vendors should guarantee code integrity and the absence of backdoors.

9.6.1.3 Analysis of Packaged Software Security Risks

The Application Administrator should assess the risk of compromising built-in security controls if a software package should be modified. Further analysis should be completed to determine if a change to the application would void future updates from the vendor, and to assess the impact if Global Eagle™ becomes responsible for maintaining the application.

9.7 Application Testing

Standards in this area cover how information security features and controls must be tested and how test data must be protected.

9.7.1 Requirements

Application security features should be reviewed with information owners and resource administrators prior to application installation and use.

Testing of security features and controls should be performed as part of application testing.

Production data should not be used for testing purposes.

9.7.1.1 Review of Application Security Features

Application security features should be reviewed with information owners and resource administrators before application installation and use. The appropriate resource administrators should be fully informed of application security controls, and user access to the applications should not be permitted until security administration controls are fully functional.

9.7.1.2 Approving Production Software

Steps should be taken to ensure that only tested and approved versions of software are accepted into the production environment, and new/upgraded software is successfully distributed without unauthorized change.

9.7.1.3 Checks Prior to Promoting Applications to Production

Before new applications and/or significant changes to existing applications are promoted to production, checks should be made to ensure that:

- Security assessments have been completed and the limitations of security controls documented.
- Segregation of duties cannot be bypassed.
- All development problems have been successfully resolved.
- The application can be supported on a continuing basis.
- Fall-back procedures have been established and tested in the event the changes malfunction.
- Approval has been obtained from the Information Owner.
- Contingency and system recovery plans are developed/updated.
- Users have been educated in use of the application.
- Resource administrators are trained in how to run the application correctly.
- Test data, accounts, usernames, and passwords are removed from production systems before becoming active.

9.7.1.4 Security Verification Tests

Testing of security features and controls should be performed as part of application testing. The security features documented during application design should be thoroughly tested. Application testing should be a joint effort of users and the development teams and should include both the manual and automated phases of the application.

Where possible Global Eagle™ should subject the software to an independent security review of the source code, especially for Internet-facing systems.

Evidence of security verification tests should be maintained for at least six (6) months and contain a classification.

Confidential. Evidence should include who performed the test, the nature of the tests performed, and the results of those tests.

9.7.1.5 Approval for Using Production Data for Testing

Production data should not be used for testing purposes unless the data has been declassified or all employees involved in the testing are pre-authorized to access the production data.

If production data is used for testing, separate authorization from the Information Owner should be obtained. This data should be depersonalized and deleted upon completion of testing, and all activity should be logged.

9.8 Secure Design

This standard establishes requirements for the design of security controls in systems.

9.8.1 Requirements

Application Security controls should be considered in order to support access restriction requirements.

The design of all systems and applications, especially those systems with high confidentiality or availability requirements, should include security and risk reduction as significant design objectives.

Application developers should include information security features in the application design itself, as information should be protected from the time it is first collected until the time it is officially disposed.

9.8.1.1 Application Controls

The following application controls should be considered in order to support access restriction requirements:

- Providing menus for controlling access to application system functions.
- Restricting user knowledge of information and application system functions, which they are not authorized to access with the appropriate editing of user documentation.
- Controlling the access rights of users (e.g., read, write, delete and execute).
- ·Ensuring that outputs from application systems handling sensitive information contain only the information relevant to the use of the output.

As necessary, the initial design documents should be revised to accommodate changes due to incorrect, inconsistent, infeasible or ambiguous security requirements identified during the design phase. The design of all systems and applications, especially those systems with high confidentiality or availability

requirements, should include security and risk reduction as significant design objectives.

Application developers should include information security features in the application design itself, as information should be protected from the time it is first collected until the time it has been disposed of officially. As part of the design phase, specific security controls should be selected. The information resources (e.g., hardware, software) required to support the selected security controls should be identified and converted to functional specifications.

User functionality (including user interface services) should be partitioned from information system management functionality.

Security functions should be isolated from non-security functions.

9.9 Application Security Controls

This standard provides guidance about the features that can be built into the application to make it a secure application.

9.9.1 Requirements

Data input into application systems should be validated to ensure the completeness and accuracy of the information processed can be confirmed.

Ensure that restrictions are implemented, to minimize the risk of processing failures that could lead to a loss of integrity.

Message authentication should be used to secure critical applications, transactions, network services and network components that execute, transmit and process TCP/IP based sensitive messages within Global Eagle's network.

Controls should be implemented to validate the output of information processed within applications.

Audit trail logs should be active at all times and protected from unauthorized access, modification and accidental or deliberate destruction on all Global Eagle™ information resources that contain Confidential or Secret information.

9.9.1.1 Input Data Validation

Data input into application systems should be validated to ensure the completeness and accuracy of the information processed can be confirmed. The following input validation controls should be implemented:

- Automated input checks (error checks) to detect out-of-range values, invalid characters, missing or incomplete data.
- Periodic review of key fields and suspicious or unusual data to confirm validity.
- · Procedures for testing the validity of input data (e.g., dual entry).
- Procedures for responding to validation errors.

9.9.1.2 Data Processing Controls

Data that has been input into applications are vulnerable to corruption through processing errors, inadvertent processing actions (e.g., accidental deletions), or through deliberate acts. Processing validation checks should be incorporated into applications to detect such corruption. The following process controls should be implemented:

- Careful placement of add and delete functions on application screens.
- Automated checks (job control checks) to prevent processing in the wrong order.
- Use of corrective programs to recover from processing failures.
- Session or batch controls to reconcile data-file balances after transaction updates.
- Hash totals to compare data after processing.

9.9.1.3 Use of Message Authentication Controls

Message authentication should be used to secure critical applications, transactions, network services and network components that execute, transmit and process TCP/IP based sensitive messages within Global Eagle's network.

Generally, sensitive messages are defined as Message Units (MUs) and other transactions that:

- Cause money to enter or leave Global Eagle™.
- Result in a change to an account/ledger balance.
- Update critical account information (e.g., account number, name, etc.).

- Are security related (e.g., interactive access such as remote login and telnet, file copying such as rcp and ftp, etc.)

During the application's security risk assessment, a determination should be made if message authentication is required.

9.9.1.4 Output Data Validation

Controls should be implemented to validate the output of information processed within applications. While input and processing controls catch most data validity errors, output validation should still occur to ensure the accuracy and completeness of the information processed. The following output validation controls should be implemented:

- Plausibility checks should be performed to test whether output results are reasonable.
- Reconciliation controls are in place to ensure the processing of all data.
- Sufficient information should be provided to determine the accuracy, completeness and security classification of the output.

9.9.1.5 Application Auditing / Logging

Application Auditing and logging should be enabled in accordance with the Security Monitoring and Response Standard.

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

Table 1: Revision History 6
Table 2: Approvals 6
Table 3: Points of Contact 6
Table 4: Associated References 7