Information Security

Information Classification and Safeguards Standard

Global Eagle™ Information Security Standard

Revision 1.0

8/10/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
8/10/2018	Igor Spektor	900.08

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Information Classification and Safeguards 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/23/2018	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	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 classification and safeguards of the Company-owned information that is electronically generated, printed, filmed, typed, stored, or verbally communicated. All information must be classified and protected according to its sensitivity and to its importance to the ongoing, legal, and effective functioning of the Company. All data in a given classification group will be controlled in the same manner, following the guidelines given here.

9 Information Classification and Safeguards Standard

9.1 Information Asset Ownership

Every Information Asset must have an owner. The owner is responsible for the security of the Information Asset. The Information Owner is the person who creates the information or is the primary user of the information.

9.1.1 Requirements

Information Owners have the responsibility to classify and label the corporate information they are responsible for, ensure appropriate safeguards are protecting the data, authorize access to those who have a business need, and remove access from those who no longer have a business need to access the information. Additionally, The Information Owner is responsible for reviewing the information classification and safeguards at least annually to ensure they are appropriate.

Examples:

1) The Head of People Services is considered the Information Owner for Employee records.

2) CFO is considered the Information Owner for Company Financial Records.

Information Custodians: Information Custodians are employees designated by the Information Owner to be responsible for maintaining appropriate safeguards established by the Information Owner. Information Custodians are also responsible for administering access to the information as authorized by the Information Owner.

Examples:

1) Administrators of the HCM system.

Information Users: Information Users are personnel authorized by the Information Owner to access the information. Information Users are responsible for using the information only for the purpose intended, and for using the safeguards established by the Information Owner.

9.2 Information Asset Inventory

Owners of business processes must ensure that an inventory is maintained of the information assets that support their business processes. This inventory must include information that is relevant for the management of the security of the information assets.

9.2.1 Requirements

The owner of the business process is accountable for the completeness and correctness of the inventory.

The inventory must contain at least the following information:

- Department.
- Business Process.
- Manager/Owner of Business Process.
- Custodian of inventory.
- Name and purpose of the information system.
- Owner of the information system.
- Information classification label.

All computer system assets shall be inventoried and valuated. Therefore all hardware and software systems must be recorded in the Configuration Management Database (CMDB) along with the attendant configurations.

9.3 Information Classification and Safeguards

Owners of Information Assets must ensure that:

Each of their Information Asset is assigned an information classification label that properly indicates its business value and criticality to the organization.

At a minimum, the labeling must be done at the Information Asset level. Nevertheless, owners may classify at more granular levels (such as sub-system, transaction type or database), with the potential to lower the overarching classification label.

This would allow specific security requirements and measures to be tailored to the classified component without having to implement them for the whole Information Asset.

The information classification label is reviewed every year or earlier if the business value or the criticality of the Information Asset has changed significantly.

The guidance and protective safeguards for each classification shall be defined in accordance with the risk valuation of such information as relevant to Global Eagle™.

9.3.1 Requirements

9.3.1.1 Security Class 1: Public

Information is deemed to be "public" if its loss or disclosure to a third party, would not harm Global Eagle™ or violate applicable information protections, mail secrecy, or other laws, and insofar as such information is readily accessible to anyone. "Public" documents (e.g., brochures), processes, and similar entities do not have to be labeled as such.

9.3.1.2 Safeguards

No safeguards, except the integrity related controls (only for the information produced by the company), are needed for information classified as Public. There are no material risks to the Company since this information is readily made available to any resource or audience who desires access or usage.

9.3.1.3 Security Class 2: For Internal Use Only

Information that is classified "for internal use only" is intended for the exclusive use of Global Eagle™ employees, contractors or affiliated entities and may not be disclosed to a third party without written authorization. The criterion for this classification is that, if disclosed to a third party, such information could be harmful to the interests of Global Eagle™ or any of its employees. This includes (but is not limited to) information regarding Global Eagle™ business processes and business interests, customer-related procedures or processes, technical descriptions, internal telephone directories, and/or inventory lists pertaining to Global Eagle™ equipment. All "for internal use only" information is to be labeled as such and can be transmitted, supplied or made accessible openly within the Global Eagle™ organization.

9.3.1.4 Safeguards

Necessary safeguards (e.g., access control with role-based access) are placed upon information classified as "for internal use only," and other than all employees, all contractors and/or affiliated entities should be made aware of its internal use requirements. Release under the terms of an approved Non-disclosure Agreement should extend these same limitations.

9.3.1.5 Security Class 3: Confidential

Confidential information means the following:

- Information that is intended solely for the use of full-time Global Eagle™ employees or approved contractors, and that such employees or contractors "need to know" in order to perform their work duties.
- Information that, if misused, could be harmful to Global Eagle's interests, particularly in regard to competitors or if such information was made public. The main types of confidential information are as follows:
    - Information regarding an aspect of Global Eagle™ operations such as operational manuals, procedural instructions, and accounting information.
    - Information that is critical to the technical or marketing success of a product or service.
    - Information regarding customers, partners, and suppliers.
    - Personal information (data), whether relating to Global Eagle's employees, customers (and their passengers) or vendors. Personal information can include any information potentially identifying an individual. It does not just include social security numbers and names. Under some jurisdictions' laws, it may include browsing histories, credit card information, physical addresses, MAC device addresses, frequent flyer numbers, etc.

9.3.1.6 Safeguards

Confidential information (in hard copy form) is to be transported in closed containers only. The containers and attendant information are to be labeled "confidential." Media containing confidential information are to be kept under lock and key.

Information owner's permission is to be obtained before confidential information is given to a temporary or contractor worker and only after such temporary worker has signed a Confidentiality / Non-disclosure Agreement (NDA). Propagation to a third party without authorization and signed NDA from the Information Owner is strictly prohibited. When any document (or digital rendition) which is classified as confidential or higher is faxed, it must be ensured that the intended recipient will receive the document personally and is authorized to receive such information.

Any confidential information transmitted outside the Global Eagle™ communication network (such as e-mail) be encrypted. All such information transfers should be secured using the existing Global Eagle™ Secure VPN and/or Global Eagle™ approved encryption system(s) in accordance with the Global Eagle™ Cryptography Standard. A record of all transmissions should be recorded and maintained with the owner of the information to ensure an audit trail of dissemination is maintained. Release under the terms of an approved NDA should extend the applicable limitations.

Confidential information at rest shall be encrypted regardless of the location of the system housing such information.

Confidential Information containing any personal identifiers such as SIN/SSN (Social Insurance/Security Numbers), Driver's License Numbers, Date of Birth, HIPAA Information, PCI (Payment Card Industry) standard relevant data shall be encrypted both at rest and in transit, regardless of the system being housed internally or externally to Global Eagle™.

Appropriate security controls must be applied to protect the confidentiality, availability, and integrity of the information processed on the systems that house the data subjected to regulations such as SOX (Sarbanes Oxley), Privacy Regulations (e.g., EU-GDPR, US Privacy Laws, etc., HIPAA).

9.3.1.7 Security Class 4: Secret

Information is classified as "secret" insofar as its disclosure could provoke a major financial loss for Global Eagle™, could severely damage the company's image, or if such information is protected by a fundamental right such as postal secrecy, intellectual property rights, or other binding requirements.

The key types of "secret" information are as follows:

- Intellectual Property relevant to Global Eagle's core strategic capability or as held in trust by an authorized Global Eagle™ contract or agreement.
- Abstracts of the transaction and inventory information of all Global Eagle™ customers.
- Information regarding a core element of Global Eagle™ business operations, such as:
    - Detailed formulations or processes concerning royalties;
    - Detailed internal electronic communication technology safeguards, configurations, or capabilities;
    - Proprietary Licensee details not made public;
    - Global Eagle™ in-process strategies or other competitive details;
    - Global Eagle™ information that is restricted by a declaration of the Global Eagle™ Board or CEO;
    - Information that is indispensable for the technical or marketing success of a product or service;
    - Descriptions of business processes over an extended period of time;
    - Material information as defined by regulatory bodies, including the U.S. Securities & Exchange Commission.

9.3.1.8 Safeguards

All of the controls that are applied to Confidential classification are applicable to the Secret classification.

In addition, the following controls must be applied:

- A recipient of Secret information may only disclose such information to full-time Global Eagle™ employees who's "need to know" such information within the context of the recipient's work duties.
- The transmission of Secret information to any full-time Global Eagle™ employee whose work lies outside the scope of the recipients is subject to the express permission of the originator of such information.
- The dispatch of any secret information via mail or courier must be comprehensively documented.

- Any Secret information that is archived electronically must be encrypted.
- Access rights to Secret information must be extremely restrictive.
- Any Secret information (data) that is transmitted must be encrypted whether internal or external.
- A record of all transfers or transmissions shall be recorded and maintained with the owner of the information to ensure an audit trail of dissemination is maintained.
- Release under the control of an approved NDA must extend the applicable limitations.

9.4 Risk Assessment

Risk assessment is the method to assure that adequate safeguards are implemented in accordance with the classification.

Owners of Information Asset must ensure that:

A risk assessment is performed on:

- New or significantly changed Information Assets.
- Components that are classified as confidential/secret.

The risk assessment must be performed prior to implementation in the operational environment.

A risk reassessment must be performed at least every year on Information Asset or components that are classified as Confidential/Secret, or earlier:

- When new security threats are identified, that may compromise the Information Asset.
- When the technical environment of the Information Asset has changed significantly.
- When, as a result of the review of the classification label, one or more security aspects have become critical.

9.4.1 Requirements

Risk assessments must be performed under control of the owner of the Information Asset. The process must at least comprise:

- An identification and description of the risks related to unauthorized disclosure, modification, and system unavailability. The object of the risk assessment must be clearly defined and should include both the technical

aspects (for example, workstation, network, server, application) and organizational aspects (for example, procedures). The identification of the risks must be based on an assessment that also addresses the likelihood and potential business impact.

- An identification and description of the security measures to mitigate the identified risks. For operational systems this concerns the implemented security measures; for systems under development, this concerns the planned security measures. The Information Asset may use security measures that are provided by the IT infrastructure. These security measures must be taken into consideration in the risk assessment for the Information Asset.
- An assessment of the residual risk. Residual risks must be approved by the owner of the business process.

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