



Media Handling and Disposal 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	900.09



6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle™ Information Security - Standard Media Handling and Disposal 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	4
2.1	COPYRIGHT	4
2.2	TRADEMARKS	4
2.3	NOTICE OF PROPRIETARY RIGHTS	4
3	Revision History	5
4	Approvals	5
5	Points of Contact	5
6	Associated References	6
7	Introduction	7
7.1	Audience	7
7.2	Assumptions	7
7.3	Owner and Contact	7
7.4	Distribution	7
8	Scope and Purpose	7
9	Media Handling and Disposal Standard	8
9.1	Security of Hard Copy Media	8
9.1.1	Requirements	8
9.1.1.1	Handling and Labeling	8
9.1.1.2	Distributing Information in Hard Copy Form	9
9.1.1.3	Storing Information in Hard Copy Form	10
9.1.1.4	Mailing Information in Hard Copy Form	10
9.1.1.5	Disposing of Information in Hard Copy Form	11
9.2	Security of Electronic Media	11
9.2.1	Requirements	11
9.2.1.1	Handling and Labeling	11
9.2.1.2	Duplicating Information in Electronic Form	12
9.2.1.3	Distributing Information in Electronic Form	12
9.2.1.4	Storing Information in Electronic Form	13
9.2.1.5	Transporting Information in Electronic Form	14



9.2.1.6	Disposing of Information in Electronic Form.....	14
10	Standard Exceptions.....	16
11	Standard Violation.....	16
12	Table of Tables.....	17



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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/8/2018	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	VP, 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
	900.00.01 - Security Policy Exception Form	900.00 - 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

All information processed at Global Eagle™ is subject to specific information (data) protection requirements. Global Eagle™ specifically handles customer information being subject to stringent information protection requirements that are mandated by law, contract, or other binding requirements. Employee information needs to be protected on a similar level. Information about business partners must be treated accordingly.

Standards in this area cover the controls necessary for handling including labeling, copying, distributing, storing, transporting, and disposing of classified information.



9 Media Handling and Disposal Standard

Handling of information (in both hard copy and electronic form), must be in alignment with the information's classification and associated safeguards requirements.

Global Eagle™ personnel must handle all non-public classified information of Global Eagle™ and its clients in accordance with Global Eagle™ Information Classification and Safeguards Standard and any applicable laws.

9.1 Security of Hard Copy Media

Standards in this area cover the controls necessary to safeguard hard copies of classified information.

9.1.1 Requirements

9.1.1.1 Handling and Labeling

Information that is obtained through employment with Global Eagle™ belongs to Global Eagle™, or to one of Global Eagle's clients, and is considered classified. Personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the handling of information in hard copy form:

- All hard copy documents that contain Confidential or Secret information should be securely handled at all times. Such information should be used in a controlled location where access is limited to personnel with a business need or will otherwise be under the physical control of an individual with authorized access to that information.
- While conducting Global Eagle™ business, employees may receive and use classified information belonging to external parties, or vice versa. Information entrusted to Global Eagle™ through contracts or agreements (including non-disclosure) will be protected according to the terms of such contracts or agreements. Questions or issues concerning such contracts or agreements should be referred to Legal and Compliance.
- When receiving Confidential or Secret information, employees should not forward this information on to others without the consent of the Information Owner. Otherwise, employees will be held accountable for any mis-distribution.

Proper labeling procedures should be followed to classify the sensitivity level of information contained within hard copy materials following Global Eagle's Information Classification Policy.



9.1.1.2 Distributing Information in Hard Copy Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines concerning the distribution of information in hard copy form:

- Classified Global Eagle™ information may not be removed from Global Eagle's premises unless there is a business requirement to do so and prior authorization has been obtained.
- Responses to inquiries about Global Eagle™ business practices, processes or significant assets should be referred to Corporate Communications.
- Disclosure of classified information about Global Eagle™ personnel to third parties should not take place unless permitted by law or by written consent of the employee. A non-disclosure agreement should be executed prior to the release of any classified information to a third party.
- Disclosure of information about current and potential customers should be strictly controlled and used only for internal business purposes. Unless the consent of the party described by the information is first obtained, all third party sale, exchange or other distribution is prohibited except as permitted by law. A non-disclosure agreement should be executed prior to the release of any classified information to a third party.
- Insider trading is the use of non-disclosed material information in the trading of Global Eagle™ stock, stock of a Global Eagle™ client, a Global Eagle™ supplier or partner, or a potential partner for profit or personal gain. Material information is information that could be considered important to an investor (e.g., financial data, potential transactions, merger and acquisitions, restructuring, minutes of use, etc.). It is in violation of the law to trade in stock if one has knowledge of such information and that information has not been disclosed to the general public. Use of such information for personal gain is subject to legal prosecution. The Securities and Exchange Commission governs disclosure of material information.
- Global Eagle™ information should not be sold or otherwise transferred to a third party unless authorized by management.
- If classified information is lost or disclosed to unauthorized parties, or is suspected of being lost or disclosed, Information Security should be notified immediately.
- The release of Confidential/Secret information requires prior authorization by the originating department's senior level management (usually Information Owner).



9.1.1.3 Storing Information in Hard Copy Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the storage of information in hard copy form:

- All information in hard copy form, classified as Confidential or Secret should be stored in a secured room, in a locked filing cabinet or desk drawer that is accessible only by authorized individuals.
- For information in hard copy form classified as Confidential or Secret, Global Eagle's employees should exercise a "clear desk" policy to reduce the risks of unauthorized access, loss of and damage to the information in hard copy form outside normal working hours. This includes clearing their personal work areas of all papers at the end of each workday, storage of these papers out of sight, and securing classified business information in locked containers.
- All Confidential and Secret documents in IN/OUT (where applicable) baskets should be stored in a locked container at the end of each business day or in an office with a locked door.

9.1.1.4 Mailing Information in Hard Copy Form

Global Eagle™ Personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the mailing of information in hard copy form:

- The mailing of Confidential or Secret information should be to a named individual and not to an office, title or location.
- The sender should use inter-company mail services or a reputable outside mail/messenger service.
- If an external mail/messenger service is used, restricted material should be sent by a means that provides verification of delivery (i.e., U.S. Mail Registered Mail, Return Receipt Requested). Due care should be exercised when selecting delivery mechanisms to areas within or outside of the United States.
- Confidential or Secret information should be wrapped or sealed in an envelope or container that is unmarked the information's classification and addressed to a named individual.
- For restricted documents, the sender should confirm, that the intended recipient received the information.



- The mailing or transmitting of technical data, software and computer programs outside of the United States may be governed by export regulations. Consult Information Security or Legal and Compliance prior to transport of hard copy media.

9.1.1.5 Disposing of Information in Hard Copy Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the disposal of information in hard copy form:

- Disposal of Confidential or Secret information should be disposed of in a manner that ensures the information cannot be reconstructed into a usable format. Papers, slides, microfilm, microfiche, and photographs containing classified information should be disposed of by cross-shredding or burning.
- The use of third-party collection and disposal services for the disposal of information in hard copy is authorized; however, care should be exercised in selecting suitable contractors that exercise adequate security controls and should have the requisite experience.
- Destruction of Confidential or Secret information should be reported to the Information Owner to permit them to update their records.

9.2 Security of Electronic Media

Standards in this area cover the controls necessary to safeguard classified information stored on electronic media.

9.2.1 Requirements

9.2.1.1 Handling and Labeling

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the handling of information in electronic form:

- All electronic media that contain information classified as Confidential or Secret should be securely handled at all times. Such media should be used in a controlled location where access is limited to personnel with a business need or otherwise, should be under the physical control of an individual with authorized access to that information.
- While conducting Global Eagle™ business, personnel may receive and use media containing classified information belonging to external parties, or vice versa. Information entrusted to Global Eagle™ through contracts



or agreements (including nondisclosure) should be protected according to the terms of such contracts or agreements. Questions or issues concerning such contracts or agreements should be referred to Legal and Compliance.

- Media containing classified information should not be left unattended in automobiles, at home or in other public areas when not in use.
- All electronic media should be handled to prevent exposure to extreme heat or cold, direct sunlight, extreme humidity and strong magnetic fields, such as those generated by motors found in fans or office heating/cooling equipment.
- When transporting backup media to a remote storage location, transportation should be performed by authorized personnel or a courier service. During movement, care should be taken to safeguard electronic media from loss, damage or destruction from both human and environmental threats.

Proper labeling procedures should also be implemented to document the classification level of information contained within electronic media as per Information Classification Policy.

9.2.1.2 Duplicating Information in Electronic Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the duplication of information in electronic form:

- The Information Owner should authorize any duplication of media containing classified information. Additionally, authorized recipients of duplicated media are responsible for controlling further duplication of this media. They may only provide copies of media to users who have a valid Global Eagle™ business need for them.

9.2.1.3 Distributing Information in Electronic Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines regarding the release and distribution (transit) of information in electronic form:

- Confidential and Secret information may not be removed from Global Eagle™ premises unless there is a business requirement to do so. This includes unencrypted information stored on portable computers or any electronic storage device.
- Global Eagle™-developed software should not be sold or otherwise transferred to a third party unless authorized by the Information Owner in



coordination with Legal and Compliance. Distribution of Global Eagle™-developed software should be documented by title, version, function, and recipient. A non-disclosure statement shall accompany the software.

- If media containing classified information is lost or disclosed to unauthorized parties or is suspected of being lost or disclosed, the Information Owner and Information Security should be notified immediately.

9.2.1.4 Storing Information in Electronic Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the storage of information in electronic form:

- All information classified as Confidential or Secret should be stored on electronic media in a locked office, a secured filing cabinet or locked desk drawer that is accessible only by authorized individuals, or be returned to a controlled media library when no longer needed. All media containing classified information will be properly stored when not in use, when unattended and when leaving the work area at the end of each business day.
- In facilities where the use of a media library is warranted due to the volume of storage required, solid state drives, magnetic tape, optical read/write media or removable disk drives containing classified information classified as Confidential or Secret should be stored in the media library. Media libraries should be secured via locked, controlled-access doors. Authorization is required for the removal of storage media from media libraries.
- All storage media should be stored away from extreme heat or cold, direct sunlight, extreme humidity and strong magnetic fields, such as those generated by motors found in fans or office heating/cooling equipment.
- Backup electronic media stored onsite will be protected in a fireproof vault or safe to protect against the effects of heat and fire. Backup media retained in off-site storage should be protected at the level of the production environment.
- Credit/debit card authentication data subsequent to authorization should not be stored including:
 - Full contents of any track from the magnetic stripe (on the back of a card, in a chip, etc.).



- Card-validation code (CVC) (Three-digit or four-digit value printed on the front or back of a payment card (for example, CVV2, and CVC2 data).
- PIN Verification Value (PVV).

9.2.1.5 Transporting Information in Electronic Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the transporting of information in electronic form:

- Physical transport of data carriers that contain information classified as Confidential or Secret may only be transferred to recipients specified by the Information Owner.
- Digital transportation of information classified as Confidential or Secret can only occur if the Information Owner grants permission and the receiving individual is given the authorization to access the data.

9.2.1.6 Disposing of Information in Electronic Form

Global Eagle™ personnel, third-party consultants, contractors, and vendors are required to adhere to the following guidelines with respect to the disposal of information in electronic form:

- All classified media should be disposed of in a manner that ensures the information cannot be reconstructed into a usable format (e.g., contract disposal service providers, etc.). Removable magnetic storage media such as diskettes and tapes that contain Confidential or Secret information or U.S. Export Controlled data should not be disposed of in regular waste containers. Tapes should be degaussed prior to discarding or reusing, and disks should be overwritten in such a manner as to cause the destruction of the classified data.
- Media containing Confidential or Secret information or U.S. Export Controlled data, which cannot be degaussed or overwritten, should be destroyed. A manufacturer-recommended degaussing product listed for the hardware or storage media should be used when degaussing. Contracting with an appropriate vendor for degaussing service may be an acceptable alternative to the purchase of degaussing equipment. If degaussing equipment is not available, the magnetic storage media can be formatted using an unconditional format. Unconditional formatting (i.e., writing over the entire disk with 1's or 0's one or more times) is formatting in such a way as to prevent the use of data recovery software to retrieve the information. Alternatively, electronic media may be destroyed by pulverization or incinerating.



Defective or damaged magnetic storage media that contains Confidential or Secret information should not be returned to the vendor who performs maintenance or repair unless the vendor is contractually required to protect such classified data. The information should first be overwritten before the media may be released to unauthorized personnel. This also applies to media on which an unsuccessful attempt has been made to copy classified information.



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	5
Table 2: Approvals.....	5
Table 3: Points of Contact	5
Table 4: Associated References	6

