Information Security

Physical Security and Environmental Controls 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	905.01

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle™ Information Security Standard - Physical Security and Environmental Controls 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/29/2018	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	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

In accordance with industry 'best practices' and to comply with numerous compliance regulations, Global Eagle™ has prepared various Information Security policies, standards, and procedures which are intended to protect the confidentiality, integrity, and availability (CIA) of our critical data and computing resources. This document describes the enterprise password standard at Global Eagle™ that shall be implemented across all systems and applications.

9 Physical Security and Environmental Controls Standard

9.1 Securing Computing Facilities

This standard establishes requirements for protecting facilities where critical computing equipment is housed and addresses controls over access, construction, and operations.

9.1.1 Requirements

9.1.1.1 Approval for Information Processing Facilities

All information processing facilities should receive appropriate management approval, authorizing their purpose and use.

Approval of the physical security designs should also be obtained from Information Security prior to utilizing the facility for information processing to ensure the relevant security controls have been implemented.

9.1.1.2 Audit and Storage of Video Monitoring

Recordings/videos from cameras used to monitor sensitive areas of computing facilities should be audited and correlated with other entries. Recordings should be stored for a minimum of three months unless otherwise restricted by law.

9.1.1.3 Access Controls

Access to facilities that are dedicated to computer processing (i.e., data centers, computer rooms) should be protected by a range of physical controls. Physical controls should protect:

- Buildings that house critical IT facilities against unauthorized access, by using locks, employing security guards and providing video surveillance.
- Important papers and removable storage media such as CDs and diskettes against theft or copying, by complying with a "clear desk" policy, providing lock-out on unattended terminals, and restricting physical access to important post/fax points.
- Easily portable computers and components against theft, by using physical locks and indelibly marking vulnerable equipment.
- Employees against coercion from malicious third parties by providing duress alarms in susceptible public areas and establishing a process of responding to emergencies.

In addition, the location of data centers should not be identified or advertised by signage or other indicators.

Access to facilities should be authorized based on the frequency and length of time needed for an individual's roles and responsibilities. All requests for permanent access should be approved by the Manager responsible for the computing facility.

9.2 Personal Control

Following requirements apply to ensure secure handling of information systems.

9.2.1 Requirements

Information, whether on paper, CD-ROM or other storage media, with confidentiality rating of critical or secret must not be left unattended. It must be kept under personal control, securely locked away and destroyed when no longer needed.

Procedures must be in place for handling classified information when no longer needed. This includes paper, CD-ROM or other media kept under personal control. (i.e., use of Clean Desk Policy.).

Process for onsite and offsite movement and storage of data, storage media must be secured and monitored.

Escalation and handling procedures for any security-related incidents with physical security aspects must be documented and audited.

9.3 Construction and Design of Computing Facility

This standard establishes requirements for structural and design features to be included in the construction of new or selection of existing computing facilities.

9.3.1 Requirements

When constructing or selecting computing facilities, the following design features should be considered:

- Computing facilities should be located in the center of buildings.
- Windows that open to the exterior of the building should be sealed.
- Building structure should be appropriate for overloading and fire risks.
- Higher floors should be avoided.
- Basements should be avoided.

- The ground floor is preferred without direct external access.
- High-risk areas should be avoided (e.g., hazardous materials, water pipes, gas pipes, propane storage, etc.).
- Holes in walls and between floors should be properly sealed.
- Elevated platforms should be used.
- Walls should extend from true floor to true ceiling.
- Hinge pins should be placed inside the computing facility.
- Doors should have sufficient strength to prevent unauthorized forced entry.
- CCTV dome camera should be placed on each corner, and as required at the center of the building and parking structure.
- CCTV fixed cameras should be placed at the loading dock, parking structure, mechanical room entry, generator room entry, and all exits.
- The fenced perimeter should be considered to enclose mechanical or generator access as required. The fence should be on two (2) inch mesh, eight (8) feet in height topped with three (3) strands of barbed wire.

IT management should ensure a low profile is kept, and the physical identification of the site of the IT operations is limited.

9.3.1.1 Environmental Concerns to be considered during Facility Construction

When constructing or selecting computing facilities, the following environmental concerns should be considered:

- Natural and artificial water positions.
- Ground quality.
- Climatic features.
- Electric and magnetic issues.
- Vibrations (e.g., fire, explosion, earthquake, etc.).
- Sufficient distance from the backup center.
- The separation between the data center and business.

9.3.1.2 Employee / Visitor Controls

The following controls should be implemented in relation to employees and visitor controls at data centers:

- A single person mantrap or optical turnstile should be implemented. Design should consider traffic flow for the proper number of these devices. Optical turnstiles are bi-directional; however, recommended design is for two (2) on each side of reception station (i.e., entry on the right, exit on the left).
- A card read in, and the card read out system should be implemented through employee controls. Attempt to pass through controls without proper card read will cause an alarm at the security desk.
- All employee entrances other than main lobby should contain a single person mantrap. Optical turnstile may be applied if the staff is on 7X24 basis or when entry is in operation.
- Loading dock entry should be controlled by security personnel. Security personnel should be present at all times when entry door to dock or loading dock doors is open.

9.3.1.3 Isolated Delivery and Loading Areas

The following security controls should be considered by Information Security when performing a risk assessment for delivery and loading areas:

- Access to a holding area from outside the building should be restricted.

- Holding areas should be designed so that supplies can be unloaded without employees gaining access to other parts of the building.
- External doors or the holding area should be secured when the internal door is opened.
- Incoming materials should be inspected for potential hazards before being moved from the holding area to the point of use.
- Incoming materials should be registered on entry to the processing site.
- Delivery and loading areas should be controlled and isolated from information processing areas to avoid unauthorized access. The security requirements of isolating these loading areas should be determined by performing a risk assessment.

When production space doors are opened, they should be under direct observation of security personnel. Remote monitoring of these doors is not acceptable.

9.3.1.4 Power / Telecommunications Cabling

Power cables within the computer installation should be protected by concealed installation, locked inspection/termination points, alternative feeds or routing, and avoidance of routes through public areas.

To minimize the threat of interception or damage, all cable and line facilities for both voice and data should be secured. Consideration should be given to the use of shielding, conduit, burial and routing away from uncontrolled areas to meet this requirement.

9.4 Visitor Entry Controls

This standard establishes requirements for protecting secured areas with appropriate entry controls to ensure that only authorized personnel is allowed access.

This also includes pass and badge controls, visitor sign-in and employee requirements to challenge any un-badged or unknown persons.

9.4.1 Requirements

All employees, third party consultants, contractors, and vendors are required to challenge and report individuals not displaying a correct access badge or are otherwise unknown.

All employees, third party consultants, contractors and vendors who do not require continued access to computing facilities in order to perform their job functions are to be considered visitors.

Visitors should be required to sign a visitor control log, and the Facility Manager should maintain control logs for at least 90 days and retain backup according to Global Eagle™ Recordkeeping policy.

Visitors to information processing facilities should receive proper authorization, should be provided a pass or badge to be displayed prominently, and provided an escort as necessary. Visitors should be asked to surrender the pass or badge before leaving the facility or on the date of expiration.

9.5 Fire Detection

This standard establishes requirements for implementing automatic systems to detect fire and smoke.

9.5.1 Requirements

All computing facilities and office areas where information systems are used should be equipped with adequate smoke and fire detection devices. These detection devices should be installed in a manner, so they are easily identifiable. The following additional controls should be implemented in data and operations centers:

- Annunciator located in the space indicating the location of the triggered head.
- Dry contact in the control panel for transmitting a summary "Smoke" signal to an alarm communication system.
- Dry contact in the control panel for transmitting a "Smoke Detection System in Trouble" signal to an alarm communication system.

- Dry contact in the control panel for initiating an alarm communication system upon receiving sprinkler flow activation and to shutdown room power and air conditioning.

Smoke and fire detectors should also be installed in all critical support facilities including electrical rooms, telephone closets, Uninterruptible Power Supply (UPS) rooms, emergency generator rooms, air conditioning rooms and similar areas.

Fire detection installations should meet federal, state and local codes for automatic fire detectors.

Fire detection systems should be connected to an alarm that will sound locally and will relay the alarm directly to the fire department or to the 24-hour security center employee who will notify the local fire department.

9.6 Equipment Maintenance

This standard establishes the requirement that equipment should be maintained to ensure its continued availability and integrity.

9.6.1 Requirements

IT management should ensure maintenance personnel has specific assignments and that their work is properly monitored. In addition, their system access rights should be controlled to avoid risks of unauthorized access to automated systems.

Preventive maintenance should regularly be performed on all information systems in conformance with manufacturer recommendations.

All maintenance tools (e.g., diagnostic and test equipment) carried into a facility by maintenance personnel should be inspected for obvious improper modifications.

All Confidential or Secret information should be purged through overwrites prior to hardware being released for off-site maintenance, unless the vendor performing the maintenance is covered by confidentiality agreement, that obliges the vendor for protection of such information and security of the equipment is ensured from source to the destination including all in-between transport/handling through auditable movement logs.

A record of all maintenance activities will be maintained and will include the date, incident, modifications, and name of the person or persons making the modifications.

9.6.1.1 Secure Disposal or Re-Use of Equipment

Damaged storage devices containing sensitive data require a risk assessment to determine if the items should be destroyed, repaired or discarded.

All items of equipment containing storage media (e.g., fixed hard disks, tapes, diskettes) should be checked to ensure that any classified data and licensed software have been removed or overwritten prior to disposal.

Global Eagle™ Media Handling and Disposal Standard should be followed.

9.7 Electrical Protection

This standard establishes requirements for protection of electronic equipment from the effects of unstable power. This includes utilization of emergency generators, uninterruptible power supply systems, power conditioning systems, emergency power-off controls and provision of dual electrical feeds.

9.7.1 Requirements

Computing facility electrical systems should be protected from electrical problems (e.g., power surges, spikes) that could cause an equipment malfunction or failure.

An Uninterruptible Power Supply (UPS) to support orderly closedown or continuous running is required for equipment that supports critical business operations. Contingency plans should cover the action to be taken if the UPS should fail. UPS equipment should be regularly checked to ensure it has adequate capacity and tested in accordance with the manufacturer's recommendations. The following is a listing of controls that should be followed in Global Eagle™ data or operations centers:

The UPS should be an online system and should incorporate:

- Auto bypass.
- Maintenance bypass.
- Online battery connection.
- Thirty (30) minute battery operation at rated load (fifteen (15) minutes with emergency generator power).
- Local panel board(s) should incorporate:
- Isolated ground bus.
- Equipment ground bus.

Alarms should incorporate:

- An indication of loss of power on supply feeder to UPS.
- An indication of the UPS system on bypass.
- Transmit a summary "UPS Failure" signal to an alarm communication system.

- If processing is to continue in case of a prolonged power failure, a backup generator should be considered. An adequate supply of fuel should be stored locally, and pre-arranged contracts with fuel vendors should be in place in the event additional fuel is needed.

9.8 Control Monitoring and Auditing

This standard establishes requirements for regular monitoring of the risk controls and periodic auditing of physical security.

9.8.1 Requirements

Risk controls (see appendix for common examples of risk controls w.r.t. physical security), once put in place; must be monitored to ensure they are both operational and effective. This monitoring should be done on a periodical basis, with the period commensurate with the control's importance.

In addition to the regular monitoring of the risk controls, physical security should be audited on an annual basis to ensure compliance with the policy. This auditing will go beyond the monitoring of the risk controls, to look at areas such as proper segregation of duties and effectiveness of anti-fraud measures.

This annual audit should be part of an overall risk-related auditing program. This audit will also provide input to regulatory procedures requiring an annual assessment of control effectiveness.

9.9 Removal of Equipment

This standard establishes requirements for ensuring that equipment, information or software is not removed from the Global Eagle's premises without approval and/or logging.

9.9.1 Requirements

Global Eagle's information resources should not be taken offsite without authorization. Unauthorized removal of Global Eagle's information resources will be considered theft.

Non-portable PCs may be removed from Global Eagle™ premises provided there is appropriate authorization from facilities management and a resource administrator.

Inventories of Global Eagle™ resources should be maintained, and spot checks should be performed to detect unauthorized removal of property. Employees, third-party consultants, contractors, and vendors should be advised that spot checks may take place.

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