Acceptable Use Policy

Global Eagle™ Information Security

Revision 1.0

6/29/2018

Global Eagle™

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
6/29/2018	Revision 1.0	Stephen Mitchell	Revision 1.0
Date			
Date			
Date			
Date			
Date			

Table 1: Revision History

4 Approvals

Name	Title	Reviewed By	Approved By	Date
Igor Spektor	VP, Head of Information Security and Compliance	Igor Spektor		6/29/2018
Dmitry Chausovsky	VP, Head of Compliance and Privacy	Dmitry Chausovsky		7/6/2018
John Gilboy	Chief Information Officer	John Gilboy		8/15/2018

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
Dmitry Chausovsky	VP, Head of Compliance and Privacy	Dmitry.Chausovsky@globaleagle.com	+1-310-740-8611

Table 3: Points of Contact

6 Introduction

6.1 Audience

This document is intended for use by Global Eagle Entertainment Inc. and its subsidiaries (Global Eagle)'s management, employees, external auditors, risk advisors, outside labor and service providers, globally.

6.2 Assumptions

This document is annually reviewed and updated, to reflect changes to Global Eagle's business processes and IT environments.

6.3 Contact/Owner

Global Eagle's Chief Information Officer and CISO-Vice President of Information Security are the points of contact for questions about this document.

6.4 Distribution

This is an electronically controlled and issued document. The latest electronic version of the document is available at (link). Users should always confirm they are using the latest electronic version of the document.

7 Acceptable Use Policy

7.1 Purpose

The purpose of this policy is to outline the Acceptable Use of Computer/IT equipment, software, fax, phone lines, mobile devices, email, and internet at Global Eagle™.

These rules are in place to protect Global Eagle employees and the Company. Inappropriate use exposes Global Eagle™ to risks including virus attacks, compromise of network systems and services, and legal issues.

Effective security is a team effort involving the participation and support of every Global Eagle™ employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to understand these guidelines and to conduct their activities accordingly.

7.2 Scope

This document applies to all employees of the company, part-time employees, and/or company employees hired on a contract basis, consultants, and other persons at the Company, including all personnel affiliated with third parties to whom the Company provides access to the Company systems or information. This policy applies to all equipment that is owned or is under control of the Company.

7.3 Policy Statement: General Use and Ownership

While Global Eagle's IT Administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of Global Eagle™. Because of the need to protect Global Eagle's network, management cannot guarantee the privacy to users for the information stored or transmitted over or on any network device belonging to Global Eagle™, even if that is a personal device owned by the employee or user.

7.3.1 Standard: General Use and Ownership

Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and FTP, are the property of Global Eagle™. These systems are to be used for principally business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations.

For security and network maintenance purposes, authorized individuals within Global Eagle™ may monitor equipment, systems, and network traffic at any time. Users have no privacy expectation in any Global Eagle™ devices, even for data thereon that is personal in nature, or any data transmitted over the Global Eagle™ network, even if personal in nature.

Global Eagle™ reserves the right to audit networks, devices and systems on a periodic basis to ensure compliance with this policy.

7.4 Policy Statement: Security of Information Resources and Proprietary Information

All Company employees have a responsibility to protect company information from unauthorized access, modification, disclosure, and/or destruction, whether accidental or intentional. All information should be clearly labeled with the appropriate information classification designation (Refer to the Global Eagle™ Information Classification and Safeguards Standard). The company has established guidelines for secure use of IT resources, which should be adhered to all the times.

7.4.1 Standard: Security of Information Resources and Proprietary Information

General Handling of Classified Information.

All information should be clearly labeled with the appropriate information classification designation (Refer to the Global Eagle™ Information Classification and Safeguards Standard).

Information for which access has been authorized may only be used for purposes identified to and authorized by the Information Owner. Copies of the information should only be made and distributed with the Information Owner's permission.

All Company information marked as Confidential/Secret should be stored and transmitted in an encrypted format when outside the control of the company network. Encrypted means that the information has been converted to a non-intelligible cipher-text format using an approved encryption algorithm and a company-owned, recoverable encryption key.The IT helpdesk can be contacted for appropriate encryption methods and tools.

When distributing Confidential/Secret information (e.g., hard copy documents, encrypted media) using public carriers, a sealed envelope or container with no external classification marking should be used.

7.4.1.1 Internet Usage

Internet access to global electronic information resources on the World Wide Web is provided by the company to assist employees in obtaining work-related data and technology.

While Internet usage is intended for job-related activities, incidental and occasional brief personal use is permitted within reasonable limits.

All Internet data that is composed, transmitted, or received via our computer communications systems is considered to be part of the official records of the

company and, as such, is subject to disclosure to law enforcement or other third parties and the requirements of the company's Record Keeping Policy.

Abuse of the company network or the Internet may result in disciplinary action, including possible termination and civil and/or criminal liability. Users have no expectation of privacy in their use of the network or use of Company's resources, and the Company may monitor, record and log that usage.

Consequently, employees should always ensure that the business information contained in Internet email messages and other transmissions is accurate, appropriate, ethical, and lawful.

The equipment, services, and technology provided to access the Internet remain at all times the property of the company.

As such, the company reserves the right to monitor Internet traffic, and retrieve and read any data composed, sent, or received through our online connections and stored in our computer systems.

Abuse of the Internet access provided by the company in violation of law or the company policies will result in disciplinary action, up to and including termination of employment. Employees may also be held personally liable for any violations of this policy.

7.4.1.2 Computer & Email Usage

Computers, computer files, the e-mail system, and software furnished to employees are the company property and are intended for primarily business use.

Employees should have no expectation of privacy even if passwords are confidential. To ensure compliance with this policy, computer equipment, software compliance and e-mail usage may be monitored.

Employees may, however, use technology resources for limited incidental personal use so long as such does not interfere with their duties, is not done for financial gain, does not conflict with company business, and does not violate any other company policy.

Email may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. This rule does not apply to company-sponsored events approved by a manager where invitations are sent to a pre-approved/defined list of participants and not broadly disseminated to the public.

Employees must exercise utmost caution when sending any email from inside the company to an outside network. Confidential/Secret information, as defined in the Information Classification and Safeguards Standard, should never be

forwarded to an outside network unless it is authorized and encrypted using an encryption method approved by the company.

Company email will not be automatically forwarded to an external destination unless approved as a Security Policy Exception using the Information Security Policy Exception Procedure.

All end-user workstations (desktop computers) should be logged off when possible, but left powered on and screen-locked, during non-working hours to allow for automatic updates of the computer software

Laptops, during non-working hours, should be shut down, and either taken home as usual process or locked in a secure location on Global Eagle premise overnight (locked drawer, cabinet, etc.) Laptops should never be left unattended in the open during non-working hours.

End-user laptops and computer workstations should be continually running approved virus-scanning software with a current virus definition database, and email attachment virus scanning should be used.

7.4.1.3 Password and Authentication Controls

As passwords, play a vital role in system security, proper policies couple with common sense must be observed at all times. Users will be held accountable for any activities performed with their individual user IDs.

The user must be aware of the proper characteristics of selecting a password (see Information Security Enterprise Password Standard) to ensure adequate protection of the Global Eagle™ and customers' information resources. Passwords must not be shared with or disclosed to another user, supervisor, co-worker or family members, including someone representing that they are from Information Technology, Information Security, People Services and, Legal & Compliance, for any reason, including events such as vacations or leaves. Passwords must never be discussed in front of other people.

Users are to refrain from writing down the password on a "cheat sheet."

7.4.1.4 Password Administration

Information Technology is responsible for the administration of user IDs and ensuring that user's passwords are within guidelines for all systems.

A supervisor that requires emergency access to a users' user ID/password, (e.g., the employee is sick, on vacation, etc.) must contact Information Technology for assistance.

At the network/system level, following password complexity criteria are implemented.

Passwords:

- Have a set expiration of ninety (90) days.
- Have to be at least ten (10) characters.
- Cannot be one of the previous twelve (12) passwords.
- Cannot contain the employee's network user ID or full name.
- Password must be constructed by the following method: It must contain at least three (3) of the following four (4) types of characters:
  - Uppercase characters (A through Z).
  - Lowercase characters (a through z).
  - Numerals (0 through 9).
  - Non-alphabetic characters (!, @, #, $, %, &, *, ?, .).

7.4.1.5 Fax/Modem Line Usage

Analog telephone lines connected to modems and fax machines or fax-modems represent a significant security vulnerability to the Company. To minimize the exposure to this threat, all analog lines must be approved by company management using an authorized request method and will be tracked, and periodically reviewed for the continued business purpose.

Periodic audits of all company analog lines will be conducted to enforce compliance with this policy.

7.4.1.6 Blogging and Social Media Activity

Blogging and Social Media Activity by employees, whether using Global Eagle's property and systems or personal computer systems, is also subject to the terms and restrictions outlined in this Policy. Limited and occasional use of Global Eagle's systems to engage in Blogging and Social Media Activity is acceptable, provided that it is done in a professional and responsible manner, does not otherwise violate any Global Eagle's policy, is not detrimental to Global Eagle's best interests, and does not interfere with an employee's regular work duties.

7.4.1.7 Use of Removable Media

Removable media is defined as: USB memory sticks/flash drives/thumb drives, memory cards, USB card readers, portable musical and media player devices, cell phones, smartphones, digital cameras with internal storage, rewritable DVDs/CDs, external hard drives, any flash based supplemental storage media and any hardware that provides connectivity to company devices through means such as wireless (Wi-Fi, WiMAX, IrDA, Bluetooth, etc.) or wired network access.

Any non-company provided hardware and software must be approved by the Information Technology department before its usage in Global Eagle™ network/systems.

7.5 Policy Statement: Unacceptable Use and Enforcement of Policy

The company strives to maintain a workplace free of harassment and sensitive to the diversity of its employees. Therefore, the company prohibits the use of computers and the e-mail system in ways that are disruptive, offensive to others, or harmful to morale. This would include the display or transmission of sexually explicit images, messages, and cartoons, as well as ethnic slurs, racial comments, jokes, or anything that may be construed as harassment, inappropriate, unprofessional or showing disrespect for others.

Company-provided Email addresses may not be used to solicit others for commercial ventures, religious or political causes, outside organizations, or other non-business matters. NOTE: This rule does not apply to company-sponsored events.

Internet access to global electronic information resources on the World Wide Web is provided by the company to assist employees in obtaining work-related data and technology. Guidelines have been established to help ensure responsible and productive Internet usage. Abuse of the Internet access provided by the company in violation of law or the company policies will result in disciplinary action, up to and including termination of employment.

Under no circumstances is an employee of Global Eagle™ authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Global Eagle-owned resources.

Employees should notify the Global Eagle™ Chief Information Security Officer or local Global Eagle People Services leader, upon learning of any violations of this policy. Employees who violate this policy will be subject to disciplinary action, up to and including termination of employment.

7.5.1 Standard: Unacceptable Use and Enforcement of Policy

The following activities are, in general, prohibited. Employees may be exempted {using proper procedures} from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may need to disable the network access of a host if that host is disrupting production services).

The lists below are by no means exhaustive, but attempt to provide a framework for activities, which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

- Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Global Eagle™.
- Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Global Eagle™ or the end user does not have an active license is strictly prohibited.
- Exporting software, technical information, encryption software, or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojans, etc.).
- Revealing your account password to others or allowing the use of your account by others. This includes family and other household members when work is being done at home.
- Using a Global Eagle™ computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Global Eagle™ account.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior notification to IT Security is made.

- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network, or account.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Providing information about, or lists of, Global Eagle™ employees to parties outside Global Eagle™.

Email and Communications Activities

- Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
- Any form of harassment via email, telephone, or paging, whether through language, frequency, or size of messages.
- Unauthorized use, or forging, of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters," "Ponzi" or other "pyramid" schemes of any type.
- Use of unsolicited email originating from within Global Eagle's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by Global Eagle™ or connected via Global Eagle's network.

Blogging and Social Media Activity

- Global Eagle's Information security policy also applies to Blogging and Social Media Activity. As such, Employees are prohibited from revealing any Global Eagle™ confidential or proprietary information, trade secrets, or any other material covered by Global Eagle's Information security policy when engaged in Blogging and Social Media Activity.
- Apart from following all laws pertaining to the handling and disclosure of copyrighted or export controlled materials, Global Eagle's trademarks, logos, and any other Global Eagle™ intellectual property may also not be used in connection with any Blogging and Social Media Activity.

Internet

- Data that is composed, transmitted, accessed, or received via the Internet must not contain content that could be considered discriminatory, offensive, obscene, threatening, harassing, intimidating, or disruptive to any employee or another person.
- Examples of unacceptable content may include, but are not limited to, sexual comments or images, racial slurs, gender-specific comments, or any other comments or images that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.
- The unauthorized use, installation, copying, or distribution of copyrighted, trademarked, or patented material on the Internet is expressly prohibited. As a general rule, if an employee did not create material, does not own the rights to it, or has not secured authorization for its use, it should not be put on the Internet. Employees are also responsible for ensuring that the person sending any material over the Internet has the appropriate distribution rights. Likewise, copyrighted and/or trademarked information should not be downloaded from the Internet to company networks or devices without obtaining prior permission in writing or having possession of a legal bill of sale or license to use such material from the owner.

7.5.2 Security Incident Reporting

Global Eagle™ is committed to providing a technologically and physically secure workplace. Global Eagle™ promotes workplace security by addressing situations in which concerns about illegal activities, misuse of resources or suspected compromise are reported and addressed in a confidential manner.

Employees are required to report any security incident involving company technology resources or assets immediately to their manager or to another manager, IT/Information Security, or officer of the company. If your manager is not readily available, you should immediately inform the aforementioned contacts so the company can take the appropriate action. Employees may report any and all concerns without fear of retaliation of any kind.

Information Security Incidents can also be reported directly to Global Eagle™ IT Helpdesk ITServiceDesk@globaleagle.com.

8 Acknowledgment

I understand that all Global Eagle™ employees have a responsibility to protect company and customer information from unauthorized access, modification, disclosure, and/or destruction, whether accidental or intentional.

I acknowledge that the Global Eagle's complete Information Security Policies are available online through the company's information security intranet portal. I further acknowledge that I have read, understand, and will comply with the Acceptable Use Policy and all of the Global Eagle™ Information Security Policies, including any authorized revisions to these policies.

EMPLOYEE'S NAME (printed):

_____

EMPLOYEE'S SIGNATURE:

_____

DATE: _____