Enterprise Password Standard

Global Eagle Information Security Standard

Revision 1.0

8/7/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
8/7/2018	Igor Spektor	900.07

Global Eagle™

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Enterprise Password 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/4/2018	Initial Draft	Stephen Mitchell	Initial Draft
8/7/2018	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		8/7/2018

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

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 Enterprise Password Standard

9.1 Password Composition

For user passwords, the following requirements apply.

Password must be composed that:

a) Is easy to remember;

b) Is difficult to guess;

c) Is a combination of alpha-numeric and special characters;

d) Is not a word in any language, slang, dialect, jargon, etc.

e) Is not based on personal information, account name, names of family or pets, birthdays, etc.

f) Is at least 10 characters long for General User accounts and, 15 characters long for Administrative / Privileged / System / Application / Service accounts.

Note

The use of so-called "first-character" passwords makes it easy to comply with the requirements. To do this, compose an easily remembered sentence (for example, "I have worked here for 2 years"), then use the first character of each word to form the password; that is, "Ihwhf2y". Such a password is easy to remember and is virtually impossible to guess.

9.2 Password History

Each Global Eagle user account(s) must have a unique password from all other accounts held by that user.

User's password cannot be the same as any of the previous 12 passwords used.

9.3 Password Communication

Passwords must not be revealed in conversations, inserted into email messages or other forms of electronic communication except for the initial password after setup.

Passwords should not be written down, stored on any information system or storage device except in accordance with any existing Global Eagle authorized password management procedures for safekeeping of passwords.

If a company employee either knows or suspects that his or her password has been compromised, it must be reported to the IT Department, and the password changed

immediately. Where available, users can also request a new password through the automatic password reset mechanism on the application.

The IT Department may attempt to crack or guess users' passwords as part of its ongoing security vulnerability auditing process. If a password is cracked or guessed during one of these audits, the user will be required to change his or her password immediately.

Initial passwords must be communicated to users either verbally or via encrypted email.

System / Application / Service Accounts password must always be stored in a password vault.

9.4 Password Age and Expiration

Initial passwords should only be valid for the first log-on attempt. Users must be forced to change the password on first use.

All user-level passwords (e.g., application user, email, web, desktop computer, etc.) must be changed at least every 90 days.

Where possible; minimum password age shall be set at one (1) day, and maximum password age shall be set at ninty (90) days. Minimum password age configuration deters intentional reuse of passwords by the user.

9.5 User Sessions Timeout and Account Lock-Out

To ensure the authenticity of the user during active sessions, a session lock must be provided, which can be activated manually by the user upon leaving the workstation, but which is also set automatically after a maximum of 15 minutes of session inactivity.

To prevent user password guessing the following measures must be implemented:

- After a maximum of five (5) consecutive unsuccessful login attempts, the user ID must be locked where after an administrator or a self-service facility must manually unlock it. It is advised that a warning is given to the user prior to the last attempt.

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