Change Management Policy

Global Eagle Information Security Policy

Revision 1.0

8/8/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
8/8/2018	Igor Spektor	902.00

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Policy - Change Management Policy 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
6/8/2018	Initial Draft	Stephen Mitchell	Initial Draft
8/8/2018	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		8/8/2018
Bob Adams	Director, Infrastructure & Global Network Services	Bob Adams		8/8/2018

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 policy provides guidance on change management including all changes, emergency maintenance, and patches, relating to infrastructure and applications within the production environment. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

9 Change Management Policy

9.1 Policy Statement

Operational change management brings discipline and quality control along with attention to governance. This formalization requires communication; the documentation of important process workflows and personnel roles; and the alignment of automation tools, where appropriate.

The defined procedure shall establish management direction and high-level objectives for organizational change management and control. It should ensure the implementation of change management and control strategies to mitigate associated risks such as:

- Information being corrupted and/or destroyed;
- Computing system performance being disrupted and/or degraded;
- Productivity losses being incurred; and
- Exposure to reputational risk.

This policy establishes requirements for recording, communicating, testing and verifying changes to information processing facilities and resources.

There must be formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.

Contingency procedures should be in place in the event that problems occur as the result of the change or upgrade.

All users, significantly affected by a change, shall be notified of the change.

While performing changes, all applicable Global Eagle™ Information Security Standards must be followed.

9.1.1 Requirements

9.1.1.1 Change Control Documentation Requirements

A formal process of documenting changes to applications, operating systems, and the network environment should exist. All change control documentation should reflect an audit trail of the change including the date and time of change, the reason for the change, the name of the person making the change, and the person or persons who authorized the change. Changes to operating system modules, tables, libraries, application software, networks, etc., should become a permanent part of the system, operations, or network documentation.

All change requests shall be logged whether approved or rejected on a standardized and central system. The approval of all change requests and the results thereof shall be documented.

A documented audit trail, containing relevant information shall be maintained at all times. This should include change request documentation, change authorization and the outcome of the change. No single person should be able to effect changes to production information systems without the approval of other authorized personnel.

All change records shall be retained for at least 12 months or in accordance with the Global Eagle™ Recordkeeping Policy.

9.1.1.2 Change Control Procedures

All information resources (networks, applications, systems, etc.) should follow formal change control procedures to ensure that only authorized changes are committed to production.

All change requests shall be prioritized in terms of benefits, urgency; the effort required and potential impact on operations.

Change control procedures should include:

- Identification and recording of significant changes, preferably in a centralized change ticket system.
- Planning and testing of changes; including user acceptance testing, where feasible.
- Assessment of the potential impacts, including security impacts, of such changes.
- Formal approval procedure for proposed changes from the application, system, or business owners.
- Communication of change details to all relevant persons [e.g., daily/weekly change management notifications].
- Fallback procedures.
- Enforcement/governance.
- Audit trail of changes.
- Configuration management and version control of all software updates.
- Notification of unauthorized modification of critical system or content files.

Contingency procedures should be in place in the event that problems occur as the result of the change or upgrade.

9.1.1.3 Emergency Changes

IT management should establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment before implementation. The emergency changes should be recorded and authorized by IT management prior to implementation.

9.1.1.4 Testing System Changes

All changes to operating system modules, tables, libraries, application software, etc., should be tested to ensure there is no adverse effect or impact on the system or application.

System Owner needs to ensure that changes are tested in accordance with the defined acceptance plan, by an independent (from builders) test group before use in the normal operational environment begins.

Changes shall be tested in an isolated, controlled, and representative environment (where such an environment is feasible) before implementation to minimize the effect on the relevant business process, to assess its impact on operations and security and to verify that only intended and approved changes were made.

Fallback/back-out plans should also be developed and tested prior to the promotion of the change to production.

9.1.1.5 Change Monitoring

All application changes will be monitored once they have been rolled out to the production environment. Deviations from design specifications and test results will be documented and escalated to the solution owner for ratification.

If feasible, all major change tickets must include a Post Implementation Review before closure.

10 Policy Exceptions

The Chief Information Security Officer must approve all policy exceptions.

11 Policy Violation

Violations of the policy in this document may subject involved employees to corrective action up to and including termination of employment.

12 Table of Tables