Backup and Restore Standard

Global Eagle™ Information Security Standard

Revision 1.0

8/8/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
8/8/2018	Igor Spektor	901.00

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Backup and Restore 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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

This Information Security Standard provides guidance on backup and restore requirements for Global Eagle™ systems and data.

9 Backup and Restore Standard

9.1 Policy Statement

It is essential to back up information (data) at regular intervals so that in the event of information processing errors or malfunctions, work can be continued based on the most recent version of the backup.

Adequate information backup/restore arrangements shall be made across all computing systems, in accordance with the business need, regulatory and operational availability requirements with an objective to minimize the loss of productivity for Global Eagle's business.

Backup should be performed for all business, financial, and critical (non-financial – i.e. email) data on a regular basis.

The procedures, scope, and schedules for backup activities are to be defined in the operational manuals of the various platforms and applications.

Information on the backup media (offline/online) must be secured in accordance with information classification. Backed-up or archived information is to be allocated the same access protection and control as the original information.

9.1.1 Requirements

9.1.1.1 Periodic Backup

Information Technology personnel should provide technical assistance for the installation of backup hardware and/or software.

System backup software should perform subsequent retries for files that are still in use at the time the backup begins. Backup systems must be configured to alert IT admin/support if the backup fails to execute.

Backup logs should be retained on the system for at least 12 months or as per Global Eagle's Recordkeeping Policy.

Backups should be monitored (automated / manual) on a regular basis, and if backups fail, an IT ticket must be created, root cause analysis (of the failure) must be performed, and resolution must be approved and documented.

Workstations attached to the network should be configured to allow the backup process to back up any critical files stored on the workstation.

Information Technology is responsible for developing, documenting, and implementing backup schedules, outlining the type of backup, interval, storage location, and the number of copies for all information resources under their control.

Below are some general guidelines for backup:

- Backup can be incremental- (daily) Full- (weekly).
- Backups can be a disk-to-disk, disk to tape, or to tape only.
- If tapes only, weekly backup tapes must be stored off-site.
- Backup rotation cycle – usually 90 days, Longer if mandated by legal and contractual requirements.
- Year-end financial data needs to be retained for seven years.
- Content data retention should be retained per contractual agreement.

Resource administrators are responsible for performing periodic backups of the information resources they have been assigned.

Backups should include, but are not limited to:

- Master files.
- Databases Transactions files.
- System programs/utilities.
- Application software Parameter settings.
- System documentation.

A minimum of one current backup copy should be maintained of each critical file.

System backup software should verify the backup that was performed by reading what was written and comparing it against the original.

9.1.1.2 Review and Testing

Periodic reviews should be conducted, at least annually, to inspect off-site storage facilities to verify compliance with retention schedules, environment protection, and security. These reviews are the responsibility of Internal Audit.

These reviews should ensure:

- Backup media is given an appropriate level of physical and environmental protection.
- Backup media can be relied upon for emergency use when necessary.

- Backup media restoration procedures are regularly checked and tested to ensure they are effective and they can be completed within the time allotted in the operational procedures for recovery. Restoration testing process sign off are documented and retained for audit evidence.

9.1.1.3 Media Storage and Disposal

All backup media must be stored in a secure location, and access restricted to authorized personnel only.

Offsite storage of backup media must be done in accordance with the Company's business requirements business continuity plan and/or other regulatory requirements, where applicable.

Backup media stored offsite must be secured, based on the backed up data's level of classification. All archival backup data stored offsite should be reflected in an up-to-date directory, which documents the date when the data was most recently modified, as well as the nature of the information.

Backup copies of the operating system and other critical information system software should be stored in a fire-rated container that is not collocated with the operational software.

In the event of any backup media disposal/destruction, Media Handling and Disposal Standard must be followed.

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