Remote Access Security 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	900.12

Global Eagle™

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle™ Information Security Standard - Remote Access Security 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/25/2018	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

This standard defines requirements for connecting to Global Eagle's network from any host. This applies to remote access connections used to do work on behalf of Global Eagle, including viewing intranet resources. Remote access implementations that are covered by this standard include, but are not limited to, ATM/frame relay, Broadband, T1, DSL, VPN, SSH, and cable modems, etc.

9 Access Management Standard

9.1 Remote Access Infrastructure

Following requirements must be met to ensure that Remote Access Infrastructure is set up in a secure manner.

9.1.1 Requirements

A remote connection must pass through a Global Eagle™ approved internet or extranet Firewall.

Only those remote access components that are related to connectivity delivery may be a part of the Firewall setup.

All data flowing between the remote access client and the Secure Perimeter, including routing information of the Inner Networks, is considered Confidential and must be encrypted in conformance with Cryptography Standard.

Any remote access infrastructure must consist of the following elements:

- An authentication service along with two (2) factor authentication enforced.
- An extranet or internet Firewall that complies with Global Eagle's standards.
- An access service managed by either Global Eagle™ or a third party that regulates user access to a system and/or application after the successful completion of strong authentication process, or a VPN server to terminate an internet VPN connection where sessions are established across the internet.

The access service serves three purposes:

- It provides the physical dial-in capabilities (if dial-in is in use).
- It acts as a network level gateway between the public network and the IP network.
- It is the place where authentication and authorization processes are performed.

The authentication server controlling the process of authentication must be located within the Global Eagle's Inner Networks.

All data flowing over remote access infrastructures is considered Confidential. Applicable rules defined in Cryptography Standard must be followed.

All access services must run on hardened systems in accordance with the Configuration Management and Security Hardening Standard.

9.2 Remote Access Client

Only Global Eagle™ Approved Remote Access Clients must be used. Security must not be allowed to depend on user-configurable security parameters on the client side.

Note

In the context of remote access infrastructure, a client is the user's system and the associated software used for remote access.

9.2.1 Requirements

The remote access server must enforce that only correctly configured clients with limited functionality are connected. This applies whether or not the user is able to change essential configuration items.

Client software must be configured in such a way that during a remote access session the only connection that can exist is with the remote access server.

Access to (parts) of the Global Eagle™ Inner Networks must be limited for all non-Global Eagle™-controlled remote clients. Unlimited access (Like Internal Private Network) to the Global Eagle™ Inner Networks at an IP level is allowed only for remote clients that are controlled by Global Eagle™.

Note

In this context, a Global Eagle™-controlled remote client would typically be a Global Eagle™-owned laptop used by a Global Eagle™ employee working from outside Global Eagle™.

All Company-owned machines being used for remote access must be kept at the current Company-approved software configuration and patch levels as specified by the IT department, including the use of the most recent anti-virus definition files.

Employees with remote access privileges must ensure that their Company-owned computer or workstation, which is remotely connected to the Company's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the Employee.

Employee's that are remotely accessing the Company network and systems must exercise the same due care, and are subject to the same information security policies, as when they are accessing these systems at work.

9.2.1.1 Approval and Authorization

All remote access must be explicitly approved by Global Eagle™ using proper access request methods in accordance with Access Management Standard.

To ensure that only authorized remote access is permitted; where possible; the application and/or data owner must explicitly permit the application and/or data to be accessed over the remote access infrastructure.

All requests for third-party remote access are subject to the Supplier Security Standard in addition to this standard. Remote Access by Third Parties shall be allowed on a need-to-know basis, to a list of selected resources only and not the entire Global Eagle™ inner network.

No service or data may be enabled over the remote access infrastructure without the owner's knowledge. The owner must explicitly allow access to these services or data.

9.3 Logging and Alerting

To ensure security and accountability in the use of remote access infrastructure, logging and altering must be implemented.

9.3.1 Requirements

Remote access logging of day-to-day operational activities is required, in order to help to detect any malicious activity.

The remote access infrastructure must provide means for applications to be able to identify if users are connected via remote access.

Note

For some applications, it may be important to be able to distinguish between users who are connected remotely or not. One way to do so is to log the user's status during the authentication and authorization process and make the status information available to applications.

All access to, and activity on, remote access infrastructure components must be logged.

Alerts must be generated for failed login attempts and unauthorized activity. Proper follow-up of alerts is required.

The logs and alerts must be stored under separate administrative control from the devices that are connected.

All logs must be reviewed periodically, at least once per month. Anomalies must be reported to responsible line management.

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