Network 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	900.10

Global Eagle™

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle™ Information Security - Standard Network 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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 provides guidance on proper security controls for Global Eagle™ network and also mandates safeguards for external connections.

Network Security Standard

8.1 Use of Network Services

Users should only have direct access to the network services for which they have been specifically authorized to use. Standards in this area cover the controls used to securely manage the risk associated with establishing connections to Global Eagle™ networks.

8.1.1 Requirements

The following controls and/or processes should be followed when granting external access to Global Eagle's network services:

- Connections should be authorized by Information Security.
- Any remote support services offered by the network service providers (e.g., ISP, telecom, etc.) should comply with Global Eagle™ security standards with regard to remote vendor support.
- All network services should pass through Global Eagle's firewall which should only allow the defined protocols and services required to provide the functionality.
- The functionality of defined protocols and ports should be analyzed as part of the risk assessment effort during the initial firewall setup. Justification and documentation should be captured for allowed risky protocols including the reason for use and security features implemented. (Use of protocols offering a high degree of functionality that may pose a risk to Global Eagle's systems should also be identified in the Risk Assessment Process).
- Appropriate controls should be put in place on Global Eagle's side of the network to minimize the risk of unauthorized access or activity.
- When possible, the connection should be initiated by the internal client to the network service supplier.
- Ensure that proper agreements are in place with information suppliers and held by Legal and Compliance.
- Firewalls should log and monitor all unauthorized activity.

8.1.1.1 Use of External Network Services

Network services provided by third parties may have unique, complex security characteristics. Business units leveraging these network services should request detailed documentation on the security attributes of all network services provided by third parties.

8.2 Inventory of Network Access Points

All access points to Global Eagle's network should be identified and documented by Information Technology.

8.2.1 Requirements

All access points to Global Eagle's network should be identified and documented by Information Technology. This includes but not limited to:

- Wireless.
- Ethernet.
- ATM/Frame relay.
- Dedicated lines.
- Remote access connections.
- Extranets.
- Internet.

Information Technology should also identify and document the applications and user groups that are accessed via the network and map the internal and external connectivity between various network segments. The information should be used by Information Technology in the design, configuration, and maintenance of Global Eagle's network.

8.3 Remote Diagnostic Ports

An information system security architecture plan should address the installation and use of remote diagnostic links.

8.3.1 Requirements

Remote maintenance ports for Global Eagle's information and communication resources should be disabled until the specific time they are needed by a vendor who has received prior authorization by Global Eagle™ personnel. Audit logs should be reviewed for all remote maintenance sessions and ports should be disabled immediately after use.

8.4 Network Segregation

This standard provides guidance for the following areas of Network Segregation.

- Isolating Servers Accessed from External Networks.
- Logical Security Domains.
- Using Switched Network Technology.

8.4.1 Requirements

8.4.1.1 Isolating Servers Accessed from External Networks

Servers which access external networks or are accessed from external networks should be logically isolated from the private Intranet.

8.4.1.2 Logical Security Domains

Networks should be segregated or divided into separate logical domains, so access between domains can be controlled by means of secure devices.

8.4.1.3 Using Switched Network Technology

Switched network technology should be utilized when possible, to prevent eavesdropping, session stealing or other exploits based on the accessibility of network traffic. A firewall should be installed at all connections from an internal to any other internal or external network.

8.5 Network Connections

This standard establishes requirements for shared networks (i.e., networks extending across Global Eagle™ boundaries) regarding the incorporation of controls to restrict the connection capability of users.

8.5.1 Requirements

Information Security should explicitly authorize all new connections to external public networks.

Personal computers, workstations, and servers should not be connected to more than one network at a time by using unauthorized means of bridging two networks.

All external access from untrusted systems or networks (i.e., Extranets) to any Global Eagle™ network should be controlled through the implementation of an approved firewall.

8.5.1.1 Approval of Connections to External Public Networks

Information Security should explicitly authorize all new connections to external public networks (i.e., Extranets). If the new connection is an additional connection to a previously certified external connection, and the connection is made following the same configuration, then no prior approval from Information Security is required.

8.5.1.2 Dual-homed Computers

Personal computers, workstations, and servers should not be connected to more than one network at a time by using unauthorized means of bridging two networks. This may include inserting more than one Network Interface Card (NIC) or using a modem while connected to another network. Dual-homed systems require approval by Information Security.

8.5.1.3 Required Use of Firewalls

All external access from untrusted systems or networks (i.e., Extranets) to any Global Eagle™ network should be controlled through the implementation of an approved firewall.

Only one method of connection to the Internet is permissible without utilizing a firewall. This method involves the use of outbound connections from a standalone computer that is not connected to Global Eagle's network.

8.5.1.4 Automatic terminal identification

Automatic terminal identification should be considered to authenticate connections to specific locations and portable equipment.

Automatic terminal identification is a technique that can be used if it is important that the session can only be initiated from a particular location or computer terminal. An identifier in, or attached to, the terminal can be used to

indicate whether this particular terminal is permitted to initiate or receive specific transactions.

8.6 Network Routing

This standard establishes requirements for shared networks (i.e., networks extending across organizational boundaries) regarding the incorporation of routing controls to ensure computer connections and information flows do not breach the access controls of business applications.

8.6.1 Requirements

Only authorized resource administrators are allowed to have physical and logical access to network routers.

Network information that should not be shared with untrusted networks should be clearly defined.

Routing Controls should be used for shared networks.

8.6.1.1 Access to Network Routers

Routing controls should be based on a positive source and destination address-checking mechanism. Only authorized resource administrators are allowed to have physical and logical access to network routers.

8.6.1.2 Network Information Not to be shared with Untrusted Networks

The following proprietary routing information pertaining to the private Intranet should not be propagated to any untrusted network:

- Routing tables.
- Domain Name Service (DNS) names.
- IP addresses.
- Network Address Translation (NAT) tables.
- Access Control Lists (ACLs).

8.6.1.3 Use of Routing Controls

Shared networks that extend across organizational boundaries require the incorporation of routing controls to ensure computer connections and information do not breach the access controls of the application.

8.7 Network Security Control Mechanisms

Standards in this area cover the use of network security control devices to protect Global Eagle™ information resources.

8.7.1 Requirements

It is the responsibility of Information Security to create and maintain Global Eagle™ Firewall Policy Configuration Document (a.k.a. Firewall Policy).

Requirements for re-authenticating active sessions after replacing a firewall should be defined.

All external access from untrusted systems or networks (i.e., Extranets) to any Global Eagle™ network should be controlled through the implementation of an approved firewall.

Define requirements for configuring routers within a firewall infrastructure.

All rules within the firewall rule base should be restricted to only allow the appropriate traffic through the firewall.

8.7.1.1 Firewall Policy

It is the responsibility of Information Security to create and maintain Global Eagle™ Firewall Policy Configuration Document (a.k.a. Firewall Policy). The Firewall Policy should state management's expectations for how firewalls should function by establishing rules for traffic coming into and going out of the security domain, and for how the firewall will be managed and updated. At a minimum, the Firewall Policy should address:

- Firewall topology and architecture (include application firewalls in front of web-facing applications).
- Type of firewall(s) being used.
- Physical placement of the firewall components.
- Monitoring of firewall traffic.
- Permissible traffic (generally based on the premise that all traffic not expressly allowed is denied, detailing which applications can traverse the firewall and under what exact circumstances such activities can take place).
- Firewall updating.
- Coordination with intrusion detection and response mechanisms.
- Responsibility for monitoring and enforcing the Firewall Policy.

- Description of groups, roles, and responsibilities for logical management of network components.
- Protocols and applications permitted.
- Regular auditing of a firewall's configuration and testing of the firewall's effectiveness.
- Contingency planning.

8.7.1.2 Re-Authenticating Active Sessions after Replacing a Firewall

In the event, a firewall fails, and a standby firewall is used, all active sessions on the firewall should be re-authenticated on the standby firewall.

8.7.1.3 Required Use of Firewalls

All external access from untrusted systems or networks (i.e., Extranets) to any Global Eagle™ network should be controlled through the implementation of an approved firewall.

Only one method of connection to the Internet is permissible without utilizing a firewall. This method involves the use of outbound connections from a standalone computer that is not connected to Global Eagle's network.

8.7.1.4 The Firewall Rule base

All rules within the firewall rule base should be restricted to only allow the appropriate traffic through the firewall. This includes, but is not limited to, restricting source and destination IP addresses, protocols, ports, and applications (i.e., outbound traffic from payment card applications should be restricted to Internet Protocol (IP) addresses within the DMZ.).

Firewall/router rule sets should be reviewed quarterly.

8.7.1.5 Configuration of Routers

The following standards should be followed when configuring routers within a firewall infrastructure:

- Source routing should be switched off on the router.
- External OSPF, RIP or other routing information protocols should be blocked.
- Amongst the ICMP protocols, only ping may be accepted.
- The TFTP protocol should be blocked.

- SNMP traffic may only be accepted by administration workstations and should not accept a public string.
- As a minimum, the router should log rejected packets.
- Remote access to the router requires strong authentication.
- Remote access to the router should be limited to internal workstations.
- Each administrator should be identified with a personal User ID.
- All changes should be documented.

8.7.1.6 \Logging and auditing of firewalls

Following sets the requirements for the logging and auditing of firewalls.

8.7.1.6.1 Logging Standards for Firewalls

The following logging and auditing standards for firewalls should be implemented:

- The firewall logs should be filed, retained for twelve (12) months, and protected from manipulation.
- Logs should contain at least the following data:
  - Successful and rejected connections to the firewall.
  - Successful and rejected connections to internal hosts.
  - Connections to external hosts.
  - Multiple, rejected connections to the same host.
- The extraction of specific information should be possible within a reasonable time and effort, possibly with a separate analysis tool.
- The firewall logs are written on the WORM (Write Once Read Many) disks and access to this data should be limited to the firewall administration and system management.
- Alarm or monitoring tools should be used to alert the appropriate resource administrator of security-related events originating from the firewall.

8.7.1.6.2 Review of Firewall Log Files

Firewall administrators should review the system logs generated from firewalls they have been assigned, on a daily basis to detect any unauthorized entry attempts or unusual behavior. The following information

should be viewed, and appropriate action should be taken if any usual activity is detected:

- Successful and unsuccessful connections to the firewall.
- Successful and unsuccessful connections to internal hosts.
- Connections to external hosts.
- Multiple, rejected connections to the same host.
- Logs should be mirrored on a separate system as "read-only" data and filed and retained for twelve (12) months [for PCI specific systems three (3) months of logs must be available online].
- Logs should be protected to prevent anyone from making changes to the stored data.

8.7.1.7 Filtering Network Traffic

Filtering of network traffic to control and restrict access across Global Eagle's network perimeter should be utilized. This filtering includes, but is n--ot limited to:

- Destination and source IP addresses.
- Ports.
- Applications.
- Protocols.
- Any non-business justified traffic that is prohibited by the Information Security Policy.

8.8 Use of De-Militarized Zones (DMZs)

The security area between two firewalls is called the De-Militarized Zone or DMZ. This standard establishes requirements for the use of De-Militarized Zones (DMZs).

8.8.1 Requirements

Global Eagle's Internet servers should always be placed in a DMZ. By placing Internet servers and any other web-facing servers in the DMZ, Global Eagle™ can reduce the potential risk of unauthorized access to its internal information resources.

Intrusion Detection Software should be implemented inside all DMZs to monitor the firewall and to monitor communications allowed through the firewall.

8.9 Network Protocols

This standard establishes requirements for the secured use of various Network Protocols.

8.9.1 Requirements

8.9.1.1 File Transfer Protocol (FTP)

The following standards for File Transfer Protocol (FTP) are applicable to untrusted relations firewall systems:

- Incoming file transfers should be treated as external connections and require approval.
- Incoming anonymous file transfer is not permitted.
- FTP configuration should implement controls for protecting data channels.
- Outgoing file transfers (e.g., to an external server) are to be handled in accordance with the Information Classification and Safeguards Standard.

FTP is used to browse directories and transfer files. Although access can be authenticated or anonymous, FTP does not support encrypted authentication. Therefore for any Non-Public class of data transfer; FTP must be done via encrypted channels as Secure FTP (SFTP), such as a Virtual Private Network (VPN), Secure Shell (SSH) or Secure Sockets Layer (SSL) sessions.

8.9.1.2 Hyper Text Transfer Protocol (HTTP)

The following standards for HTTP are only applicable to untrusted relations firewall systems:

- Port 80 should be blocked against external access.
- Alternative ports such as 8080 should be protected against external access.
- All HTTP servers that can be accessed externally should be in a De-Militarized Zone (DMZ).
- Proxying and/or stateful inspection should be used for all connections to and from the public Internet and other untrusted networks.
- Rules of the Acceptable Use Policy apply when accessing internal objects.

8.9.1.3 Trivial File Transfer Protocol (TFTP) Restrictions

The use of Trivial File Transfer Protocol (TFTP) on information systems is prohibited unless a formal exception request is authorized by Information Security.

TFTP is a file transfer protocol with no file-browsing ability and no support for authentication.

8.9.1.4 Non-Essential Services

The following standards are applicable for untrusted relations firewall systems:

- All non-IP protocols should be blocked by the firewall.
- SNMP traffic should be blocked in both directions.
- NTP traffic is only permitted to a central, internal timeserver.
- The use of "Berkeley r" protocols by the firewall is generally forbidden.
- The firewall should prevent the following protocols from entering:
  - NFS.
  - RPC portmapper.
  - NIS.
  - TFTP.
  - X11.
  - Finger.
- UDP packets are only permitted in conjunction with a "status-creating" proxy.
- All unused network services (e.g., Telnet) and unnecessary shells and interpreters (e.g., Perl) should be disabled on all WWW host machines.

8.9.1.5 Domain Name Service (DNS)

The following Domain Name Service (DNS) standards are applicable to untrusted relations firewall systems:

- Internal hostnames and IP addresses are classified as "internal" and should not be visible externally.
- Queries to non-existent host names should be logged and rejected.
- A split DNS configuration should be used.

- External DNS entries are limited to servers externally accessible.
- No queries may be forwarded to internal DNS services from external DNS services.

8.9.2 Wireless LAN Infrastructure

All wireless network devices connected to Global Eagle™ internal networks must use a wireless LAN infrastructure that complies with requirements of this standard.

8.9.2.1 Requirements

All Un-approved Wireless LAN infrastructures are considered untrusted and cannot exist within the internal Global Eagle™ network that is protected by the Secure Perimeter.

Access to Global Eagle™ connected systems and/or data must pass through the following process steps:

- The user authenticates to the wireless device, in line with user authentication requirements of Access Control Standard.
- The user enables the wireless device within range of an Approved access point, at which time the wireless card automatically attempts to associate with the access point and obtains an IP address, for example via DHCP.
- The wireless access point connects the wireless device to a VPN gateway.
- The device establishes an encrypted "tunnel" between the device and a system connected to Global Eagle™ internal network, either the wireless LAN gateway or an internal device. This tunnel may only be established after successful authentication of the user and/or device. The wireless LAN gateway may only allow data transfer through the gateway after successful authentication.
- Data may only be transferred through the gateway by means of an established encrypted VPN tunnel. VPN termination must take place either in the wireless LAN gateway or on a device somewhere else in Global Eagle™ network.

After successful completion of these steps, the user can access an application using the same access protection mechanisms of the application as have been implemented for users accessing the application using a hard-wired workstation.

Peer-to-peer connections between wireless devices are not allowed when there is also a connection with the Global Eagle™ network. For wireless point-to-point

connections between Global Eagle™ locations, two wireless gateways will be involved.

8.9.3 Wireless LAN Approval

All wireless LAN implementations require approval by Global Eagle™ Information Security Department.

8.9.3.1 Requirements

- Wireless LAN designs need to be approved by Global Eagle™ Information Security Department.
- Wireless devices used by Global Eagle™ employees for obtaining access to data and/or systems connected Global Eagle™ internal networks need type approval by Global Eagle™ Information Security Department.
- Wireless access points need to be registered centrally within the local IT organization.
- Business units must assume responsibility for identifying and preventing network access via unregistered (rogue) wireless access points.

8.9.4 Wireless LAN Security

All wireless devices that are used by Global Eagle™ employees for obtaining access to data and/or systems connected to Global Eagle™ internal networks must conform to the following Global Eagle™ security standards:

- Workstation Security Standard.
- Cryptography Standard.
- Access Control Standard.
- Remote Access Security Standard.

Authentication and network/transport layer encryption should be used for Wireless connections to protect wireless access to the information systems.

8.9.4.1 Requirements

Authentication and network/transport layer encryption should be used for Wireless connections to protect wireless access to the information system. (e.g., WPA2, IPSEC VPN or SSL/TLS).

Wireless LAN gateways either implement a VPN gateway itself or are only allowed to make connections to a VPN gateway if this gateway is implemented on another platform elsewhere in the network.

All data transferred between the wireless device and the wireless gateway must be encrypted. The form of encryption used must conform to Cryptography Standard.

Local IT management and Global Eagle™ Information Security Department may shut down wireless LAN access points if security vulnerabilities have been identified in wireless LAN designs and/or components.

Due to a vulnerability in the hardware implementations of the IEEE 802.11 wireless protocol, the IEEE 802.11, the 802.11b and low-speed (below 20Mbps) 802.11g wireless devices must not be used for availability critical services.

9 Standard Exceptions

All standard exceptions must be approved by the Chief Information Security Officer.

10 Standard Violation

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

11 Table of Tables