Information Security and Data Privacy

Access Control Standard

Global Eagle™ Information Security Standard

Revision 1.0

7/31/2018

Effective date *(update for each revision)*	**Document Owner**	**Document ID**
7/31/2018	Igor Spektor	900.01

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Global Eagle Information Security Standard - Access Control 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
5/8/2018	Initial Draft	Stephen Mitchell	Initial Draft
7/31/2018	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		7/31/2018
				7/31/2018

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 standard provides guidance on authorizing and authenticating users before granting them access to information resources. Users should be positively authenticated and authorized prior to being granted access to information resources. Access based on an employee's role should be limited to the minimum necessary to perform their job function.

Controlling access to the Company's information assets is the foundation upon which all other information protection efforts are built. Therefore, access to the Company's network, systems, and information must be strictly controlled. It is the responsibility of all Information Custodians, under direction from the Information Owners, to implement the safeguards described here.

9 Access Control Standard

9.1 User Notification

Prior to access, the user must be notified that access is only allowed for authorized users.

Note

Where feasible it is advised to also implement user notification in systems and applications.

9.1.1 Requirements

Users should be informed regarding the purpose of their access to the information asset and required to limit their use of the information asset to the purpose defined. User activity should be monitored to enforce appropriate usage, and users should be made aware that their activity is being monitored.

Prior to access to the network, a clear message must be displayed to the user indicating that access is only allowed for authorized users. The user must confirm acceptance of this message.

EXAMPLE:

NOTICE Login is only allowed for authorized users.

9.2 Identification

Access must be based upon a valid ID. All users accessing Company information assets must be positively identified using a unique identifier, usually in the form of an account or login name.

Generic/Shared Accounts –The accounts that are used by more than one person are only allowed by exception, using the Policy Exception process. The accounts that are used by more than one person are only permitted by exception, using the Policy Exception process.

Administrative / Privileged Accounts – These accounts are defined as those user accounts which afford the account holder the ability to administer account management, maintenance, monitoring, or removal, or which allow the read, write, modify or delete privilege to file systems for which they are not the Information Owners, but have been designated as Information Custodians for the purpose of performing administrative functions, or which afford the account holder the ability to set and/or

modify the operational or security configuration of the system, application, or service account.

System / Application / Service Accounts – These Accounts are defined as the accounts used by any system related service, individual application or utility or application configured to run under its own credentials irrespective of user authentication, Accounts used to communicate between two different applications in mutual authentication process or accounts used for impersonation. These accounts should strictly be used by subjected application/system only and not by any individual.

9.2.1 Requirements

For all employees, contractors or service providers that desire access to an information resource or network, proper access request procedures must be followed to define/establish the identity.

EXAMPLE: A request/form should be completed by Human Resources or the user's immediate manager and forwarded to Information Technology for review and approval. Enrollment Process is used to establish a user's identity, and anticipated business needs to information and related information resources before assigning a unique user identification number (User ID) to the user.

During the login process, an ID must be provided by the user or the system/application that requests access. The validity of the provided ID must be checked against the access control administration tool/process. Access must be denied when the ID is not known or is blocked.

Requirements for User IDs

Uniqueness — User IDs should be unique across all systems and forever connected with the single user to whom it has been assigned. To minimize the risk that dormant access permissions are accidentally inherited by a new user, there should be no reuse of any User IDs.

Usage — User IDs should not be utilized by anyone except the individual to whom the IDs have been issued. Users are responsible for all activity performed with their User IDs. All users with access to the information resources should use a User ID that has been specifically assigned to them. Users should not perform any activities with User IDs belonging to others.

Non-Disclosure — User ID lists should not be published unless they are part of an approved addressing scheme (e.g., email address book, corporate directory structure). In these situations, User ID information should be adequately protected against disclosure.

Requirements for Generic, Group or Shared IDs:

Generic, Group or shared IDs are not permitted unless permission has been granted by the security policy exception procedure. All the compensating controls must be documented in exception request.

Requirements for Default IDs:

Default User IDs shipped with software must be used in an approved manner reviewed by Information Security.

Default parameters should be set when creating new identifiers.

All default, pre-set, or temporary passwords and accounts assigned internally should be set to a unique value per user and changed immediately after first use.

Vendor-supplied defaults should be changed during installation of third party software on the network. This includes, but is not limited to the following:

- Passwords.
- Elimination of unnecessary accounts / user IDs (i.e. guest).
- Simple Network Management Protocol [SNMP] community strings.
- Access keys (e.g., passphrases, Wi-Fi access keys, etc.).
- Service Set Identifier (SSID).
- Disabling of SSID broadcasts.
- Enabling of Wi-Fi Protected Access (WPA) technology for encryption and authentication when WPA-capable.

9.3 Authentication

Authentication is the verification of identity by a system, based on the presentation of unique credentials to that system. The unique credentials are in the form of something the user knows, something the user has, or something the user is (e.g., fingerprint or other biometrics). Authentication contributes to the confidentially of data and the accountability of actions performed on the system, by verifying the unique identity of the system user. Each user must be authenticated using an approved authentication method.

For access to systems/applications or data, the minimum level of user authentication is a user ID and password.

Strong password with two-factor authentication is always required for access via internet or wireless connections unless access is limited to a specific isolated computer environment that only gives access to functions or data that are classified as Public.

Where login is performed by systems/applications, using a system or application ID, sufficient controls must be in place to ensure appropriate authentication. The minimum level of authentication is a system/application ID and password.

Systems and applications can be accessed through a Reduced/Simplified/Single Sign-On (SSO) facility. In these cases, the requirements as mentioned above remain valid.

The sign-on credentials must be forwarded by the SSO service to the systems/applications in a secure manner. When SSO is implemented for a business critical system/application, the consequences of this must be addressed in the risk assessment for that system/application.

9.3.1 Requirements

To verify the identity of a user with a password, the system/application must prompt the user for a password. The system/application must check the validity of the entered password in relation to the user ID. Account credentials on publicly accessible systems should always be encrypted.

Passwords are an essential aspect of computer security. They are the front line of protection for user accounts and systems. A poorly chosen password may result in the compromise of the company's entire corporate network. As such, all company employees (including contractors, vendors and any other individual or entity with access to company systems) are responsible for immediately assigning secure passwords to all Company accounts created for their use.

For user passwords the following requirements apply:

User rules:

Choose a password that:

a) Is easy to remember;

b) Is difficult to guess;

c) Is a combination of alphabetic and non-alphabetic (numeric/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 ten (10) characters long for General User accounts and, fifteen (15) characters long for Administrative / Privileged / System / Application / Service accounts.

Keep passwords confidential:

- Never disclose it to or share it with others.
- Never use passwords suggested by someone else; immediately change initial or reset passwords that are received from others (for example, from security administration) after receipt.
- Avoid keeping a record of passwords.
- Do not use facilities such as "remember my password boxes."
- Ensure that passwords only are stored in encrypted form. This also applies to PCs, smartphones/tablets, cell phones, USB-pluggable drives or other portable devices.
- Immediately change the password after (suspected) disclosure.
- Do not re-use recently used passwords or passwords that are known to be compromised.
- Do not use the same password for access to company systems/applications and non-company systems/applications, because the security of the passwords in non-company systems/applications is beyond the control of Global Eagle™.
- All passwords are to be treated as confidential Company information and are not to be written down or shared with anyone else, including co-workers. Passwords should never be revealed over the phone, via email, or in any other manner, and any requests for your password should be re-directed to Global Eagle Information Security Team. Requests to have a forgotten password reset shall require the verification of previously obtained "secret" information provided by the user.
- Change passwords regularly, at least every 90 days.

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 two (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.

System controls:

- Enforced change at first usage of the initial password.
- Enforced change after 90 days of the unchanged password.
- Disabling of initial passwords that are not used within one week after creation.
- Enforced controls on initial or changed passwords:
  - at least ten (10) characters long for General User accounts and, fifteen (15) characters long for Administrative / Privileged / System / Application / Service accounts.
  - A combination of alphabetic and non-alphabetic (numeric/special) characters, or a check against dictionary words.
  - Not the same as any of the previous 12 passwords used.
- No display, logging or printing of passwords in plain text.
- Encrypted storage and transport of passwords.
- Enforced controls on initial or changed passwords.
- Check against unwanted password values (e.g., all the same characters).
- After a password change confirmation of the new password by the user.

For two-factor user authentication the system must require the user to be authenticated using two securely implemented mechanisms out of the following list:

- Something the user knows (such as a user password).
- Something the user possesses (such as a token, smart card, OTP-One Time Passcode/PIN received through the separate channel).
- Something the user is (such as a biometric scan, fingerprint, iris scan, voice print).

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.

Users must not leave an open session unattended and must manually activate the session lock or shut down the session when leaving the workplace.

The reason for failed authentication must not be communicated by the system to the user, to prevent giving clues to the user about which aspect of the login process failed."

For system/application authentication, the preferred method is using PKI certificates. When the use of certificates is not available, a system/application strong password is the minimum implementation for system/application authentication. The requesting system/application must present the password to the target system/application for verification. When the authentication fails, a limited number of restarts of the verification process must be allowed.

Note

A retry, similar to user authentication use case, is not applicable for system/application authentication as mistakes during the password entry are not likely. However, the authentication can fail due to technical problems. To solve this, restart of the process must be supported.

For a system/application password the following requirements apply:

Passwords must only be stored in locations prescribed by systems/applications.

- If passwords are stored in plain text (for example, within scripts, configuration files, registries or memory) they must only be accessible by system administrators.
- If passwords are stored encrypted it must be prevented that a single person knows the entire password, for example by the implementation of a system generated password or by a password composed from dual control input.
- When the password is suspected to be compromised it must be changed (regular enforced password change is not required).
- System / Application / Service Accounts password must always be stored in a password vault
- When key staff who knows the password, leaves the organizational unit, the password must be changed.

9.4 Authorization

Access must be limited to authenticated IDs, in accordance with granted access rights. It is the Information Owners responsibility to determine appropriate access privileges based on the user's role, function, and need-to-know or need-to-do.

9.4.1 Requirements

Where possible, levels of access should be divided into separate security groups, and one or more security groups should be associated with defined roles. These roles and security groups should be reviewed at least annually by the Information Owner, and adjusted as needed.

Information owners are responsible for reviewing and approving all requests for access to information resources and applications for which they have been assigned responsibility. System administrators are then responsible for granting the level of access that has been approved by the Information Owner.

All User Access Request forms/tickets should be retained for a period of at 18 months and contain the classification of 'Confidential'.

System/application IDs must be disabled for interactive login, for example, disabled for use on consoles.

Requirements for review and revocation of Access privileges:

- User accounts must be audited on a monthly basis. A list containing the following information is generated and reviewed by the Information Security Operations Manager:
  - New accounts.
  - Removed accounts.
  - Accounts inactive for >60 days.
- User Accounts that are inactive for 60 days will be disabled and moved to a holding area within the directory structure. All accounts in the holding area will be deleted after 30 days unless marked as Regulatory in the description field.
- Administrative accounts will be reviewed by the IT Operations Manager (currently Director End User Support) and approved on a monthly basis.
- Access privileges granted to general users should be reviewed by information owners at least annually to determine if access rights are commensurate with the user's job duties. Evidence of account and privilege reviews that documents the review occurred, who conducted the review, and what action (if any) was taken should be maintained for a period of twelve (12) months or as per Global Eagle's document retention policy.
- Access privileges granted to privileged users should be reviewed by the Information Owner at least every three (3) months (preferably just prior to Quarter-end) to ensure the privileged access level is still valid.

- Business managers are responsible for reporting changes in user duties or employment status for all employees under their supervision to Human Resources. Human Resources is responsible for reporting changes to information owners responsible for the information resources to which the involved user has access. Resource administrators should promptly revoke all unnecessary access privileges.
- Information owners should promptly report all changes in user duties or employment status, to the Resource Administrator responsible for the User IDs associated with the involved personnel. Resource administrators should promptly revoke all unnecessary access privileges.

9.5 Logging and Auditing

Relevant details regarding successful and unsuccessful system access attempts must be logged to facilitate an audit trail. Logs must be reliably retained in accordance with agreed procedures and retention periods. Audit trails should be reviewed on a periodic basis to ensure compliance with the policy.

9.5.1 Requirements

All account activity should be logged and proper audit trails maintained for all access to information assets. Audit trails should be reviewed on a yearly basis to ensure compliance with the policy. Administrative access involving the use of high-level system privileges should be reviewed on a frequent basis, using real-time alerting of inappropriate access where possible.

For all user/ system activities at least the following must be logged:

- User ID.
- Date and time, login /logout.
- If possible: workstation ID/network area.
- Results (successful/rejected).

Access to Audit logs must be read-only and restricted to authorized personnel.

Audit logs must be retained for a period of at least 12 months or longer as required for legal or regulatory reasons.

Reports must be generated for security violations to the application/system and must be reviewed.

Activities which update production user information must be logged and reported for verification of input.

There must be documentation on how violations will be addressed.

9.6 Alerting and Monitoring

Exceptional unsuccessful access attempts to systems/applications that are critical from confidentially and/or integrity standpoint, must be identified and must trigger an alert. Alerts must be followed by an effective response.

Administrative access involving the use of high-level system privileges should be reviewed on a frequent basis, using real-time alerting of inappropriate access where possible.

9.6.1 Requirements

All access and security logs must be monitored on a regular basis.

Exceptional security violations (security alerts) must be reported in an incident management system for; a real-time response for example, via a security console. A comprehensive record must be maintained. The reported alert must give enough information for an effective response:

- Violation type.
- Involved User ID(s) and resources.
- Date and time.
- A number of failed access attempts.
- Types of the requested access.
- If possible, the location from where the attempts were made.

Note

The criteria for exceptional security violations differ per system. For example, exceeding an exceptional limit of security violations per minute, hour, day, etc. might indicate a systematic hacking attack. This limit could depend on the number of users, the type of authentication, the time period and other circumstances.

Incident management procedures must be documented and implemented to ensure an appropriate response. It must include notification/escalation procedures to notify stakeholders in the event of an intrusion.

9.7 Prevention of Password Guessing

Measures must be implemented to prevent successful password guessing.

9.7.1 Requirements

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

- For access to systems/applications: After a maximum of 5 unsuccessful login attempts the user ID must be locked where-after it must be manually unlocked by an administrator or a self-service facility. It is advised that a warning is given to the user prior to the last attempt.

9.8 Password Management Systems

The password management systems should provide effective mechanisms to ensure Global Eagle's password composition and usage policies are followed.

9.8.1 Requirements

This standard sets the requirements for authentication mechanisms and must be followed to the closest degree. Any exception for not adhering to these must be weighed based on risk assessment and be approved by policy exception procedures.

For access to any critical information resource the password management systems should:

- Enforce the use of individual passwords to maintain accountability.
- Allow users to select and change their passwords.
- Enforce alphanumeric password composition rules.
- Force users to change temporary passwords at first login.
- Require re-authentication before permitting a user to re-access an information resource after a period of inactivity.
- Maintain a record of previous user passwords to prevent re-use.
- Not provide specific feedback to the user if any portion of the login information is entered incorrectly.
- Only indicate login failure after both the identifier and authentication information has been entered.
- Not display or allow printing of passwords on the screen while being entered.
- Encrypt and store password files separately from systems data.

- Lock, disable or delete vendor accounts after product installation.
- Not display system or application identifiers until the login process has been completed.
- Not provide help messages during the login process that would aid an unauthorized user.

10 Standard Exceptions

The Chief Information Security Officer must approve all standard exceptions.

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