Data Privacy and Information Security Incident Response Plan

Revision 1.0

6/27/2018

Effective date *(update for each revision)*	Document Owner	Document ID
7/6/2018	Igor Spektor Dmitry Chausovsky	900

6100 Center Drive, Suite 1020

Los Angeles, CA 90045

USA

This Incident Response Plan 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Global Eagle™ claims copyright in this documentation as an unpublished work, revisions of which were first licensed on the date indicated in the preceding notice.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
06/27/2018	Revision 1.0	Stephen Mitchell	Initial Draft

Table 1: Revision History

4 Approvals

Name	Title	Reviewed By	Approved By	Date
Igor Spektor	Head of Information Security and Compliance	Igor Spektor		7/2/2018
Dmitry Chausovsky	Head of Compliance and Privacy	Dmitry Chausovsky		7/2/2018

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
Dmitry Chausovsky	VP, Head of Compliance and Privacy	Dmitry.Chausovsky@globaleagle.com	+1-310-740-8611

Table 3: Points of Contact

6 Introduction

6.1 Audience

This document is intended for use by Global Eagle Entertainment Inc. and its subsidiaries (Global Eagle)'s management, employees, external auditors, risk advisors, outside labor and service providers, globally.

6.2 Assumptions

This document is reviewed (at least annually) and updated as appropriate.

6.3 Owner and Contact

No material part of this document is to be altered without the agreement of Global Eagle Chief Information Officer (CIO), Chief Information Security Officer (CISO), and Head of Compliance and Privacy. All updates to this document must be implemented using proper change control.

6.4 Distribution

This is an electronically controlled and issued document. The latest electronic version of the document is available at (link). Users should always confirm they are using the latest electronic version of the document.

7 Key Terms

The following are some key terms and definitions used throughout this document:

Company: Company or the Company refers to Global Eagle™.

Personal Data: Any information that can be used to identify, contact, or locate a single individual.

Sensitive Personal Data: Personal information that could cause significant harm to an individual or the Company, is not adequately protected or used, is not collected for a lawful purpose or is lost or disclosed to unauthorized persons. Sensitive Personal Data includes Personal Identifiable Information (PII) data that can be used to commit fraud or identify theft, as well as information that has been specially designed as such by applicable laws and regulations.

Incident: for purposes of this plan, an "Incident" includes, but is not limited to the following:

- Any actual or suspected occurrence in which an unauthorized person acquires or accesses an individual's confidential Information from the Company, or when the Company has otherwise lost control or possession of such confidential Information, and such information is not encrypted, redacted, or secured by a method or means which makes the data unusable.
- Any unauthorized use, access, or compromise of Personal Data or Sensitive Personal Data.
- Compromise of information integrity (damage to data or unauthorized modification).
- An attack that causes one of the Company's web-facing services to be unavailable to the Company or its vendors or customers.
- Infection of systems by unauthorized or hostile software.
- Reports of unusual system behavior when the root cause is not otherwise known.
- A stolen or lost laptop, tablet, mobile device, or other portable electronic storage media.
- Theft or loss of physical files containing Personal or Sensitive Personal Data.
- The hacking of a website, database, or system.
- The unauthorized downloading of confidential Information to a personal device.
- Content theft, broadcast disruption, denial of service, website defacement, or social media hijacking.

Incident Response Team (IRT): IRT is a team of assigned business and functional stakeholders and/or technical experts. The IRT is authorized to take appropriate steps deemed necessary to contain, mitigate, or resolve privacy and/or information security incident. The team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings under the direction of CIO/CISO/Head of Compliance and Privacy as necessary.

8 Incident Response Plan

8.1 Purpose

This document describes the Data Privacy and Information Security Incident Response Plan (Incident Response Plan).

The Company must reasonably safeguard the Company's systems, confidential information/content owned by the Company, personal data of its customers and clients from any intentional or unintentional use or disclosure that violates the Company policies.

The purpose of this Incident Response Plan is to ensure the following:

- The management of Data Privacy and Information Security incidents for Global Eagle is effective and efficient to meet operational and compliance requirements.
- Defined lines of responsibility for Global Eagle business and functional stakeholders are identified for the incident response and incident management processes.

8.2 Policy Statement: Incident Response

The CIO, CISO, and Head of Compliance and Privacy are jointly responsible for the implementation of the Incident Response Plan processes and the communication of the Incident Response Plan policy statements within the Company.

The Incident Response Plan is designed to guide and support actions in the event of data privacy and/or information security incident. The security and availability of data, systems, and other resources are vitally important to the Company. Implementing and following this Plan should assist the Company to comply promptly with its legal obligations as well as reduce the risk of an incident that could cause serious harm to affected individuals and the Company's reputation and finances.

8.3 Identifying and Reporting an Incident

The identification and reporting of an Incident may be triggered by a variety of events, both internal and external to the Company including Company's personnel, law enforcement, or media reports, and for a variety of reasons.

Incidents can be reported, identified via the following methods:

- Reported to the Company's management and/or designated personnel responsible for handling data security incidents (example: Chief Information Security Officer, Head of Compliance and Privacy).
- Via the Ethics Point hotline (Toll-free +1-866-422-3580).
- Global Eagle Entertainment IT Service Desk (ITServiceDesk@globaleagle.com).

- Via IT Service Management Ticket System.
- Global Eagle Entertainment System Monitoring (Alerts, Notifications & Reports).

Levels of incidents can be identified by automatic system alerts & reporting within monitoring systems and alerted and reported when anomalies arise and/or based on regular reporting intervals. These incidents will be managed and resolved internally within Global Eagle.

8.4 Incident Response Process

Incident Response Process (IRP) begins immediately after the reporting of an incident. Analysis of the incident will take place by an IRT lead, and that will determine whether IRT activation is appropriate.

Once an incident is identified to be information security or privacy-related incident; within 24 hours, the Company will engage a pre-defined Incident Response Team (IRT). The Chief Information Security Officer (CISO) will be the central point of contact for IRT. However, any IRT member can be contacted to invoke the Incident Response Process. Any incidents involving loss or a potential loss of employee's and/or customers' personal data must be reported to the Company's VP, Head of Compliance and Privacy.

8.4.1 Identifying an Incident

Along with the definition of an Incident as described under Key terms above, the following statements may be used as a guide to assist with determining the nature of an incident:

- "Any event that results in loss or damage to the Company or client information assets." This may involve harm or unauthorized access to the Company or client information assets that impact the confidentiality, integrity or availability of those assets, including loss and unauthorized release of Personal Data of the Company's employees, customers and other parties, whose Personal Data the Company collects and processes.
- A virus or worm becomes active within the Company or client-computing environment causing network outages, infection of other machines, or loss of productivity to multiple individuals.
- "An observation of a potential threat to the Company or client information assets." Examples include:
    - An activity or issue that may expose the Company or a client information asset to a threat.
    - An activity or issue that may indicate an incident but is not an incident in and of itself.
- "Any event or action that is initiated within the Company network that damages clients, partners, vendors or other entities." Examples include:

  - Any unauthorized action that is meant to probe or discover information about a client, partner, vendor or other entities computing environment, or;
  - Any action that harms, or is intended to cause harm, to the information assets of clients, partners, vendors or other entities, or;

- "Any event, action, or situation that may negatively impact the Company or its client's image, integrity or business position." This statement is designed to allow the IT and the Company Management to respond to incidents that may not be specifically "information security" in nature but require immediate response to lessen the impact of the incident.

Issues that do not pose an immediate threat should be reported and processed through the normal management and response channels.

8.4.2 Incident severity levels

Three severity levels of data privacy and information security incidents are defined as follows:

High Risk

- Multiple systems or customer information have been or are being compromised or disrupted. Levels of performance (function, production) may be seriously affected.
- Intruders might execute arbitrary commands on system servers.
- The ability to execute commands on a system generally implies the ability to cause a denial of service or to gain unauthorized data access.
- Identification of an unauthorized and "rogue" wireless access point.

These breaches allow intruders to establish a base of operations within the system from which to capture network traffic and spread their span of control. This level of breaches should be corrected immediately.

Medium Risk

- A single system or customer information has been compromised.

Medium level breaches permit some level of unauthorized data access or denial of service. These breaches can be leveraged to allow intruders to gain complete control of system resources eventually. Medium level breaches should be corrected as soon as possible.

Low Risk

- System threatened or data affected is minimal or contains no sensitive information (such as information classified as public or internal use, in

accordance with the Information Classification and Safeguards Standard) and can be easily restored.

Low-level vulnerabilities permit reconnaissance activities that allow would-be intruders to collect network topology and configuration information, including active IP addresses, active network services, valid usernames, etc. These vulnerabilities do not directly lead to unauthorized access, but they should be corrected to make it difficult for intruders to enter the system. Some data access vulnerabilities that are relatively minor, unintentional, or for which exploit tools are readily available, are also classified as Low-level breaches.

Note

For Data Privacy related incidents; High Risk should be assumed at the onset unless advised otherwise by Head of Compliance and Privacy.

8.4.3 Incident Response steps for IT Service Desk

1. Follow standard ticket management process and create an IT support incident ticket in service desk platform and categorize it as a security incident (if available further subcategories may be used as appropriate, for Information Security and Data Privacy Incidents).
2. Identify severity of the breach according to the levels defined above.
3. Identify system(s) affected.
4. Escalate High & Medium Risk incidents to IRT and manage Low-Risk Incidents within IT Service Desk, keeping CISO informed of the ticket progress. If the incident involves any confirmed or suspected, Personal Data or Sensitive Personal Data compromise or loss, also inform Head of Compliance and Privacy.
5. Contact appropriate Systems Administrators to take the necessary actions in coordination with the assigned Incident Owner and IRT.
    - For High/Medium Risk Incidents copy the Senior Director, User Support Services, and CISO. CISO will assign an Incident Owner. If the incident involves any confirmed or suspected, Personal Data or Sensitive Personal Data compromise or loss, Incident Owner must engage Head of Compliance and Privacy.
    - For High-Risk Incidents, Incident Owner shall engage IRT and initiate an hourly conference call for status and progress. This call shall continue until canceled by, CISO, CIO, or Head of Compliance and Privacy (if it involves Data Privacy related incidents).

- For Medium Risk Incidents, Incident Owner shall engage IRT and keep Senior Director, User Support Services, and CISO, informed of the progress via email/ticket updates.

8.4.4 Incident Response Steps for IRT

There are a number of steps and stages that must be taken by reacting to an incident appropriately.

8.4.4.1 Investigate

After being notified of an incident, the IRT will perform an initial investigation and determine the appropriate response, which may be to initiate the Incident Response Plan. If the Incident Response Plan is initiated, the IRT will investigate the incident and initiate actions to limit the exposure of compromised data and, in mitigating the risks associated with the incident.

The IRT will work to determine and document the cause, nature, and scope of the Incident, including the following:

Scope:

- The date, time, duration, and location of the Incident.
- What systems were affected, if any?
- What type of personal data and/confidential Information was or is reasonably believed to have been affected or compromised.
- The magnitude of files, records, databases, or devices that were or are reasonably believed to have been affected or compromised.

Nature:

- How the Incident was discovered, by whom, and any other known details including the method of intrusion;
- Entry or exit points; paths taken; to compromised systems;
- Whether data was deleted, modified, viewed, and so forth; and whether any physical assets are missing.

Affected Individuals: Who the affected persons are (if known), where they reside (if known), and, for each person or category of persons, what information has been affected or compromised.

Note

Depending on the type and format of data compromised, the Company may need to work with customers to ascertain what data, including confidential Information, was affected.

Preliminary Risk Analysis:

- Determine best and worst case scenarios, and what is reasonably likely to happen to the data that was compromised.
- Determine whether other systems are under the threat of immediate or future danger.
- Determine whether external parties are aware of or are likely to become aware of the Incident.

If necessary, in consultation with Legal, the Company may engage specialized third parties to assist in conducting the analysis at the direction of counsel for purposes of a legal investigation.

8.4.4.2 Initial incident containment and response actions

Make sure that no one can access or alter compromised systems.

- Isolate compromised systems from the network and unplug any network cables – without turning the systems off.
- If using a wireless network, change the SSID (Service Set Identifier) on the wireless access point and other systems that may be using this wireless network (but not on any of the systems believed to be compromised).
- Preserve all logs and similar electronic evidence, e.g., logs from the firewall, anti-virus tool, access control system, web server, application server, database, etc.
- Perform a back-up of the systems to preserve their current state – this will also facilitate any subsequent investigations.
- Keep a record of all actions that members of the IRT take.
- Stay alert for further indications of compromise or suspicious activity in the environment, or that of the Company's third parties.
- Seek advice before you process any further payment card transactions. (Only applicable in case of Payment Card Industry (PCI) related systems).
    - If possible, gather details of all compromised or potentially compromised payment card numbers (the 'accounts at risk').

8.4.4.2.1Preserve Evidence

The IRT keep a record of the steps taken to contain the data incident, and will take care to:

- Preserve the confidentiality, integrity, and availability of systems and information.
- Preserve evidence, including through the use of a proper chain of custody.
- Safeguard information related to the investigation (including information that the investigation is occurring).

When appropriate, Legal will issue a litigation hold to preserve the Company's information relating to the incident. As additional facts are uncovered, legal in consultation with the IRT will re-evaluate whether a litigation hold is advisable.

8.4.4.3Inform

Once the IRT has carried out their initial investigation of the incident:

- The Incident Owner will alert the IRT Lead and Head of Compliance and Privacy (for Data Privacy related Incidents).
- The Incident Owner and/or the IRT personnel responsible for communications will inform all relevant parties. This may include the acquirer (in case of PCI related breach), local law enforcement, and other parties that may be affected by the compromise such as the customers, business partners, or suppliers. This also includes the personal data breach notification contacts, as applicable to the incident under investigation. Any notifications to outside parties related to incidents must be done in consultation with Legal and Compliance.

8.4.4.3.1When Breach Notification Is Required

Legal and Head of Compliance and Privacy must be consulted for appropriate communications outside the company, but as general guidance, the following incidents may require notification to individuals under contractual commitments or applicable laws and regulations:

- A user (employee, contractor, or third-party provider) has obtained unauthorized access to personal information maintained in either paper or electronic form.
- An intruder has broken into the database(s) that contain personal information on an individual.

- Computer equipment such as a workstation, laptop, CD-ROM, or other electronic media containing personal information on an individual has been lost or stolen.
- A department or unit has not properly disposed of records containing personal information on an individual, in accordance with the *Media Handling and Disposal Standard*.
- A third-party service provider has experienced any of the incidents above, affecting the organization's data containing personal information.

The following incidents may not require individual notification under contractual commitments or applicable laws and regulations providing the organization can reasonably conclude after an investigation that misuse of the information is unlikely to occur, and appropriate steps are taken to safeguard the interests of affected individuals:

- The Company is able to retrieve personal information on an individual that was stolen, and based on our investigation, reasonably concludes that retrieval took place before the information was copied, misused, or transferred to another person who could misuse it.
- The Company determines that personal information on an individual was improperly disposed of, but can establish that the information was not retrieved or used before it was properly destroyed.
- A laptop computer is lost or stolen, but the data is encrypted.

Note

Any notifications to outside parties related to incidents must be done in consultation with Legal and Compliance who together with the business will determine whether such notifications are legally mandated and/or appropriate in case of non-mandatory notifications. Any law enforcement contact can be done ONLY under the direction of Legal and Compliance. Legal and Compliance should review any reports or communications with law enforcement, state regulatory agencies, and credit reporting agencies. The IRT also should consult Legal and Compliance before responding to any law enforcement requests to see internal documents.

Additionally, consideration should be given to any contractual notification obligations the Company might have with affected customers, individuals. A determination regarding insurance notification obligations to the Company's insurance carrier(s) must also be given as part of the incident review and resolution.

8.4.4.3.2 Internal communications

If directed by Legal and Compliance, all internal written reports and communications about a data incident should be clearly identified with the notice: "Privileged & Confidential, Attorney-Client Privileged, and Prepared at the direction of counsel/Attorney Work Product."

8.4.4.4 Maintain Business Continuity

The IRT will engage with operational teams in the business to make sure that the business can continue to operate while the security incident is being investigated.

8.4.4.5 Resolve

With prior knowledge of Legal and Compliance, the CISO or a CISO delegate from IRT, or Head of Compliance and Privacy for data privacy incidents, will liaise with external parties, including the acquirer (in case of PCI relevant breach), law enforcement, etc., to ensure appropriate incident investigation (which may include on-site forensic examination) and gathering of evidence, as is required.

The members of the IRT will take action to investigate and resolve the problem to the satisfaction of all parties and stakeholders involved. This will include confirmation that the required controls and security measures are operational and Incident Tracking Grid is updated.

The Incident Owner will report the investigation findings and resolution of the security incident to the appropriate parties and stakeholders as is needed.

8.4.4.6 Recovery

The IRT Lead or Incident Owner will authorize a return to normal operations once the satisfactory resolution is confirmed.

The IRT will notify the rest of the business that normal business operations can resume. Normal operations must adopt any updated processes, technologies, or security measures identified and implemented during incident resolution.

8.4.4.7 Review

The IRT will complete a post-incident review after every incident and update Incident Tracking Grid as needed. The review will consider how the incident occurred, what the root causes were and how well the incident was handled. This will help to identify recommendations for better future responses and to avoid a similar incident in the future.

Changes and updates that may be required include:

- Updates to the Incident Response Plan and associated procedures.

- Updates to the security or operational policies and procedures.
- Updates to technologies, security measures, or controls.
- The introduction of additional safeguards in the environment where the incident occurred.

The CISO/CIO/Head of Compliance and Privacy will ensure that the required updates and changes are adopted or implemented as necessary.

8.4.5 Escalation Matrix

At any point in time, during the incident response process, delays for any reason could result in an increase of the severity and/or impact of the incident. Therefore following time-based escalation matrix must be used by the assigning party (or incident owner) for any/all of the steps to ensure the assigned tasks are timely addressed, and incident resolution is progressing.

Time to respond (total time passed from the start of the task assignment)	Escalation Level	Escalated to
8 hours	1	Any IRT Member
13 hours	2	IRT Lead
16 hours	3	CISO and Head of Compliance and Privacy
18 hours	4	CIO

Table 4: Escalation Matrix

8.4.6 Incident Response Deliverables

The following items are deliverables that are produced as a result of the Incident Response process.

Incident Response deliverables, as applicable:

- Incident Record.
- Logged Incident Records.
- Restored Service.
- Productivity Improvements.
- Incident Record Closure.
- Incident Review.
- Notification to appropriate Authorized User(s).
- Requests for Change via Change Management (as necessary).
- Incident data provided to IT Management (as necessary).
- Incident reports (as necessary).
- Updated Incident Tracking Grid (Link).

8.5 Tools

Tool	Purpose	Tool Owner
IT Service Management Ticketing System	▪ Recording the details of incidents. ▪ Production of Incident and incident related metrics and management reports for internal use to improve the restoration process and the Incident Response process. ▪ Configuration management database.	Global Eagle Entertainment
Conference Bridges	▪ Communications amongst all technical resolver groups. ▪ Communications amongst all stakeholders.	Global Eagle Entertainment
Incident Tracking Grid	To maintain a master repository for all incidents and associated details, stored in the Incident Response Portal: **Error! Hyperlink reference not valid.**	IRT

Table 5: Tools

8.6 Roles and Responsibilities

The Incident Response Team (IRT) is comprised of the following:

Role*	IRT Responsibility	Name	Email	Telephone
CISO	Incident Response Lead	Igor Spektor	Igor.spektor@globaleagle.com	954-401-9155
CIO	Incident Response Escalation Lead	John Gilboy	John.Gilboy@globaleagle.com	562-201-7210
Infrastructure	Incident Response Technical Lead	Bob Adams	Bob.Adams@globaleagle.com	954-289-7985
Applications	Incident Response , Application Lead	Kumar Manish	Kumar.Manish@globaleagle.com	310-779-6815
EVP and General Counsel	Handling of any legal questions/issues relating to security incidents	Stephen Ballas	stephen.ballas@globaleagle.com	310-740-8618
Compliance VP, Head of Compliance and Privacy	Contact for any incidents involving loss or unauthorized release of personally identifiable information	Dmitry Chausovsky	dmitry.chausovsky@globaleagle.com	310.740.8611 (O) 310.74.6689 (C)

Role*	IRT Responsibility	Name	Email	Telephone
[Other Personnel With A Role In Business' Incident Response Plan, e.g., Suppliers, Managed Service Providers, E-commerce Hosting Providers]	[MSSP Specific Incident Response Role, To Be Specified]	[Insert Details]	[Insert Details]	[Insert Details]

Table 6: Roles and Responsibilities

Note

Select the personnel and roles appropriate to the size and operations. Staff may hold more than one role.

9 External Contacts

External Party	Contact Name (if known)	Email	Telephone
Visa Europe Data Compromise Team		datacompromise@visa.com	+44 (0) 20 7795 5031
Visa Inc Incident Response - US		usfraudcontrol@visa.com	(650) 432-2978
Visa Inc Incident Response - Canada		CanadaInvestigations@visa.com	(416) 860-3090
Visa Inc Incident Response Latin America & Caribbean		lacrmac@visa.com	(305) 328-1713

Table 7: External Contacts

10 Table of Tables