Aspen Group, Inc. (AGI)

## Approval and Ownership

The **Chief Operating Officer** is the authorized decision maker who can either approve or deny changes to this document.

## Revision History

This document shall be reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date of Change** | **Section** | **Description of Change** | **Change Authority** |
| 1.0 | March 2019 | Full Document | Initial Release | Gerard Wendolowski |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Enforcement

Any personnel found to have violated any policy or process shall be subject to disciplinary action, up to and including termination of employment.

# Incident Response Overview

The VP, Systems shall be responsible for establishing all security incident response and escalation procedures.

The process will address the following at a minimum:

* Roles, responsibilities, and communication and contact strategies in the event of a compromise;
* Notification requirements;

The plan shall include a review / lessons learned process. Using information from completed incidents, modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

## Purpose

An incident response plan defines all of the actions required in the event of a data breach or other security related incident.

## Scope

This document applies to all personnel accessing or utilizing sensitive data in computer resources, data communication networks, or other information technology infrastructure resources owned or leased; including any other corporation or agency having connectivity to the network are subject to these Information Security policies.

## Roles and Responsibilities

The Senior IT Manager or the VP, Systems may serve as the Incident Coordinator. The Incident Coordinator is responsible for resolving the incident in accordance with the Incident Response Policy.

## Data Breach

The term ‘breach’ means the unauthorized acquisition, access, use, or disclosure of sensitive information which compromises the security or privacy of such information.

The term ‘breach’ does not include any unintentional acquisition, access, or use of sensitive information by an employee or individual acting under the authority of a covered entity or business associate if such acquisition, access, or use was made in good faith and within the course and scope of employment.

Refer to the appendix titled “Data Breach Incident” for details of the action items related to a breach of sensitive data and the notification process.

## Data Breach Notification

The Chief Executive Officer will determine an appropriate notification process.

## Data Loss

Data loss is an error condition in information systems in which information is destroyed by failures in storage, transmission, or processing.

## Release of Information

Control of information during the course of a security incident or investigation of a possible incident is very important. All release of information must be authorized by the Chief Executive Officer or the Chief Operating Officer.

## Types of Incidents

A security incident is a violation or imminent threat of violation of security policies, acceptable use policies, or standard security practices. Examples of incidents are as follows:

* **Denial of Service** – an attack that prevents or impairs the authorized use of networks, systems, or applications by exhausting resources.
* **Malicious Code** – a virus, worm, Trojan horse, or other code-based malicious entity that successfully infects a host.
* **Unauthorized Access (Breach)** – a person gains logical or physical access without permission to a network, system, application, data, or other IT resource.
* **Loss of Equipment or Media** – removable equipment (laptop etc.) or media is lost or stolen.
* **Inappropriate Usage** – An employee or contractor has:
  + Violated the employee handbook; or
  + Has compromised physical or data security; or
  + Has shared or released sensitive information without proper approval.

# Incident Response Process

All initial reports of what appears to be a serious incident must be reported to the Chief Operating Officer.

The Incident Coordinator will investigate whether an incident actually occurred, the severity of the incident, and the urgency of a response. All reported incidents that are designated as legitimate incidents will be promptly classified according to their severity and urgency. Incidents may require reclassification as further information comes to light.

The IncidentCoordinator will decide which methods and processes will be followed in response to an incident.

The Incident Coordinator will determine if the incident should be escalated to the Executive Team. All decisions about the involvement of law enforcement personnel must be made by the Chief Executive Officer.

The Incident Coordinator will track all relevant events and tasks associated with the incident, providing status to all appropriate parties. A history of all incidents shall be maintained.

## Review

It is imperative that the Company learns from incidents that occur in order to reduce the likelihood of an incident from reoccurring and to improve the response process. The review phase will examine the effectiveness of the response, and if necessary, update security policies and take preventative steps to ensure the incident cannot happen again.

Approved By:

|  |  |  |
| --- | --- | --- |
| Name: | Michael Mathews | Joseph Sevely |
| Title: | CEO | CFO |
| Signature: |  |  |
| Date: |  |  |

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# 

# Appendix: Virus Incidents

|  |  |
| --- | --- |
| **Task** | **Actions / Comments** |
| Notify | Notify the Senior IT Manager as soon as possible. If unable to reach him/her within 10 minutes, notify the VP, Systems and your manager.  The Senior IT Manager will then be responsible for notifying other appropriate personnel. |
| Log | The Senior IT Manager will keep a log of their actions taken. |
| Isolate | Isolate infected system(s) as soon as possible. |
| Identify | Try to identify and isolate the suspected virus related files and processes. |
| Contain | All suspicious processes should be halted and removed from the system. |
| Inoculate | Implement fixes and/or patches to inoculate the system(s) against further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. |
| Return | Before restoring connectivity, verify that all affected parties have successfully eradicated the problem and inoculated their systems. |
| Follow Up | Refer to the appendix titled “Follow Up Analysis and Review” |

# Appendix: Follow Up Analysis and Review

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. If applicable, a set of recommendations should be presented to the appropriate management levels. A security incident report should be written by a person designated by the Chief Operating Officer and distributed to the appropriate personnel.

|  |
| --- |
| **Task** |
| Review what caused the event. |
| Review how the Incident Coordinator resolved the Incident. |
| Identify any outstanding tasks or requirements. |
| Determine if all appropriate individuals have been notified. |
| Review learnings and determine how to improve. |

# Appendix: Data Breach Incident

|  |  |
| --- | --- |
| **Task** | **Actions / Comments** |
| Notify | Notify the Chief Operating Officer, VP, Systems and your manager as soon as possible. If unable to reach him/her within 10 minutes, notify the VP, Technology.  The designated Incident Coordinator will then be responsible for notifying other appropriate personnel. |
| Log | The Incident Coordinator will keep a log of their actions taken. |
| Identify | Identify the source of compromise and the time frame involved.  Review the network to identify all compromised or affected systems.  Examine the appropriate system and audit logs for each system affected. Document all IP addresses, operating systems, system names and other pertinent system information |
| Contain | Do not alter a compromised system in a way that would destroy evidence.  Possible steps include:  1) Isolate the affected systems from the network. 2) Modify firewall rules to prevent system access or stop network traffic.  3) Change passwords or disable compromised accounts.  4) Monitor systems and the network for signs of continued intruder access.  5) Examine other hosts on the network segment or hosts that share a trust relationship. |
| Prioritize | Identify what must be recovered and establish the priority of each item. Determine the steps that will be taken to recover the environment |
| Collect/Preserve | Decide if preservation of evidence or critical data is required, if so: 1) Make backups of the affected systems. 2) Make copies of system and application log files that contain evidence. |
| **Notification** | |
| Notify | The Incident Coordinator will communicate regularly with the Chief Operating Officer during an investigation, who will keep the Chief Executive Officer aware of the situation as events progress. |
| Internal User | If an Internal User (employee, contractor, consultant, etc.) was responsible for the breach, contact the VP, Human Resources for disciplinary action and possible termination. |
| **Recovery** | |
| Restore | The recovery steps may include the following: 1) Identify and mitigate all vulnerabilities that were exploited. 2) Eradicate malicious code. 3) Harden and patch affected operating systems and applications. 4) Reinstall the affected systems from scratch and restore data from backups if necessary. 5) Verify/update virus protection system. |
| Verify | After the incident has been resolved the affected systems shall be tested to prevent any recurrence. |
| Reactivate | After the issue has been resolved, the systems have been verified and tested; the systems may be put back into production. |
| Notify | The Incident Coordinator will summarize the incident and notify the Chief Operating Officer. |
| Follow Up | Refer to the appendix titled “Follow Up Analysis and Review” |