STUDY ABROAD ASSOCIATION

IR PLAN - 360 GLE™

Approval Date: April 1st, 2023

INTRODUCTION

This document outlines the procedures to be followed in the event of a security incident or data breach involving our web application. It defines the roles and responsibilities of the Incident Response Team and the procedures to be followed in the event of a security incident.

INCIDENT RESPONSE TEAM

The Incident Response Team (IRT) is responsible for the coordination and management of security incidents. The team is composed of the following members:

- Incident Manager: Responsible for coordinating the incident response process and ensuring that all necessary steps are taken to contain the incident and minimize its impact.
- IT Security Officer: Responsible for overseeing the security of the web application and its underlying infrastructure.
- System Administrator: Responsible for the maintenance and operation of the web application.
- Legal Counsel: Responsible for providing legal guidance and ensuring compliance with relevant laws and regulations.
- Public Relations Officer: Responsible for managing the organization's external communications regarding the incident.

INCIDENT IDENTIFICATION

The IRT must be notified as soon as possible when a security incident is suspected or detected. Incident identification can be triggered by various sources, including but not limited to:

- Suspicious activity reported by users
- Malware or virus detection
- System or application error messages
- Any other indicators of a security breach

INCIDENT CONTAINMENT

Once an incident has been identified, the IRT must take immediate action to contain it. The following steps should be taken:

- Notify the appropriate personnel (e.g., network administrators, system administrators, IT security personnel)

INCIDENT ANALYSIS

The IRT must analyze the incident to determine its scope, nature, and cause. The following steps should be taken:

- Gather all available information about the incident
- Determine the extent of the damage and the potential impact on the organization
- Identify any compromised data and the affected systems

INCIDENT RESPONSE

Based on the analysis of the incident, the IRT must determine the appropriate response. The following steps should be taken:

- Develop a plan for mitigating the incident
- Take steps to restore normal operations
- Notify any affected parties (e.g., users, customers, partners)
- Provide guidance to affected parties on how to protect themselve

POST-INCIDENT REVIEW

After the incident has been resolved, the IRT should conduct a post-incident review. The purpose of this review is to identify areas where improvements can be made to the incident response process. The following steps should be taken:

- Document the incident and the response process
- Identify any weaknesses or gaps in the response process
- Develop a plan to address any identified weaknesses or gaps
- Review the incident response plan regularly to ensure its continued effectiveness

In the case of any unusual activity please immediately notify:

techsupport@studyabroadassociation.com

STUDY
ABROAD
ASSOCIATION

WWW.STUDYABROADASSOCIATION.COM