Security Response Plan Policy

Issue Statement

Affinity Partnerships, LLC. shall respond to computer security-related incidents in a manner that protects its own information and helps to protect the information of others that might be affected by the incident.

A security incident is defined to be any adverse event that threatens the security of information resources. Adverse events include compromises of integrity, denial of service, compromises of data -- sold or used in an unauthorized fashion, loss of accountability, or damage to any part of the system.

Organization's Position

Affinity Partnerships, LLC. has established a Service Application (SA) Computer Security Incident Response Capability (CSIRC) to address computer security incidents, including theft, misuse of data, intrusions, hostile probes, and malicious software. When an incident occurs, the supervisor must provide a verbal report to the ISSO within one working day after the incident. A written preliminary report must be submitted within two working days. Within five working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty days, a weekly status report must be submitted to the ISSO.

Applicability

OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems requires all organizations to have an incident response capability and to share information concerning common vulnerabilities and threats. Affinity Partnerships, LLC. Automated Information Systems Security Program Handbook outlines the CSIRC components and steps to establish a CSIRC. The SA system will comply with the following rules outlined in this document.

Roles and Responsibility

Chief Technology Officer shall:

- publish and maintain policy guidelines for handling SA computer security incidents,
- provide management oversight of the process for handling SA computer security incidents, and
- immediately inform Affinity Partnerships, LLC. CEO and senior management of significant incidents (major compromise of data, denial of service).
- prepare policy guidelines for establishing and implementing the CSIRC,
- notify the CEO and senior management of significant incidents and response plan,
- work with law enforcement, the users and/or system administrators, and the network manager/administrator to formulate an initial response plan[1],
- work with the users and/or system administrators, and the network manager/administrator to review and if necessary modify response plan;
- update senior management,

- determine if incident follow-up is needed,
- submit reports[2] to the CTO, CEO and senior management,
- inform the Federal Computer Incident Advisory Capability (FedCIRC) if the incident is computer security related.

Department Managers shall:

- communicate to employees the SA incident response requirements outlined in this policy,
- contact the CTO within one working day after the incident,
- notify management of significant incident and response plan,
- work with law enforcement, the users and/or system administrators, the network manager/administrator, and the CTO to formulate an initial response plan,
- update management, and
- ensure reports are prepared and submitted within established timelines to the CTO.

User/System Administrator shall:

The User or System Administrator should perform the following if there is a suspicion that something is amiss[3]:

- investigate briefly,
- if suspicion is ungrounded, log and share knowledge with CTO and networking manager/administrator,
- if suspicion is confirmed or indeterminate, confer with supervisor, CTO and networking manager/administrator,
- start an event log by noting date and time of all actions,
- take snapshot of pertinent files within the first half hour of incident investigation,
- identify risk to system or information,
- confer with CTO and networking manager/administrator,
- implement response plan within forty-five minutes of incident discovery,
- notify management of significant incident and response plan,
- monitor and study situation, and
- assist supervisor in preparing preliminary and final report.

Networking Manager/Administrator shall:

- work with the users and/or system administrators, and the CTO, to formulate an initial response plan,
- assist when necessary to evaluate and mitigate incident, and
- review response plan and if necessary assist in modifying the plan.

Compliance

The CSIRC Standard Operating Procedures are mandatory and are designed to standardize the incident handling and reporting.

Supplementary Information

- Affinity Partnerships, LLC. Automated Information Systems Security Program Handbook

- OMB Circular A-130, "Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems"

Points of Contact

Tim McClanahan- email: Timm@affinityps.com Mobile Number: 208.406.9144