Tier 1 Control Standards (State-Wide)

Incident Planning and Management

Standard ID
IOT-CS-SEC-132

Published Date
6/15/2007

Effective Date
6/15/2007

Last Updated
5/19/2017

Next Review Date
5/19/2018

Policy
15.0 Response Planning (RS.RP)
15.1 RS.RP-1
15.1.1 Response Plan

Purpose
It is required that state agencies apply responsible protective measures to Indiana government assets, foremost of which is sensitive information. Indiana government is of size and complexity that incidents are inevitable. Therefore it is necessary for state agencies to consider and plan for incidents before they occur.

Scope
IOT Supported Entities

Statement
Security incidents include, but are not limited to the compromise of information from: stolen or lost computing devices (laptop, PC, blackberry), malware (virus, worm, and Trojan horse) detection, unauthorized use of computer accounts and computer systems, as well as complaints of improper use of Information Resources as outlined in the Information Resources Use Agreement (IRUA).

Agencies must report security incidents using the attached form to the Chief Information Security Officer (CISO – IOTCISO@iot.in.gov). Reporting incidents permits the state to assure the best possible defensive actions are used, that necessary communications occur, promotes collaboration and information sharing with state agencies, and collect statewide information on the types of vulnerabilities that are being exploited, frequency of attacks and cost of recovering from an attack.

Below are the requirements for handling information security incidents:

Awareness and planning – Agencies must take time to assess the likely incidents that could impact their organization. Steps to take include the following:

- The first priority is to recognize measures available that minimize the incident likelihood and aggressively implementing mitigating actions.
- Understand the nature of potential incidents and take actions that would minimize the extent of damage from an incident.
- Understand the role of the State’s information security incident response team (ISIRT). Contact the CISO regarding questions on the role of ISIRT in handling incidents.
For each potential circumstance, identify the individuals that need to be involved in handling the incident. Have all necessary contact information including phone, cell phone, and email addresses (work and home) documented to enable a prompt response. Be sure to include contacts from other agencies that could potentially play a role in effectively dealing with the incident (Governor’s Office, IOT, State Personnel, State Police, Inspector General and Attorney General).

Establish internal procedures for dealing with incidents. Assure that communication requirements for each potential incident are included.

Train staff on the risks identified and the plans for dealing with incidents.

Test – Agencies shall select a potentially serious incident and run through the scenario. For effectiveness the fact that it is a test should be shared minimally. Test outcomes should be assessed and necessary adjustments made to improve effectiveness. Particular attention should be paid to the effectiveness of documented procedures and adjustments made based on test experiences. Testing should occur on a regular basis.

Handling an incident – In the event of an incident, the agency should invoke their tested procedures. The following steps are essential to dealing with an incident:

- In case of theft or burglary, file a police report on the stolen property.
- Contact ISIRT (through the State CIO or CISO) immediately allowing them to assist your team with the incident.
- Clearly identify the scope of the incident including the source of the compromise and the information resources at risk.
- Minimize damage - if the incident is ongoing or if the vulnerability exploited remains, immediately involve the appropriate technical resources.
- Assess damage and circumstances – collect and maintain the facts about the circumstances. Focus data collection and analysis on identifying the who, what, when, where and how of the adverse event.
- Gather evidence - collect information with proper documentation and ensuring its safeguard. If the incident could be prosecuted in court, the following special precautions regarding chain of custody must be taken:
  o Ensure evidence is gathered appropriately and not altered;
  o Ensure evidence is accounted for at all times;
  o Verify the passage of evidence from one party to another is fully documented
  o Verify the passage of evidence from one location to another is fully documented
- Communications – report complete information to parties requiring notification (this could include state agencies, the Attorney General, businesses, and citizens). Communications should be conducted carefully, on a need to know basis, and information related to the compromise should be deemed “confidential” during the security incident investigation.

Returning to operations – Agencies will want to return to normal operations as quickly as possible. Before doing so agencies must completely evaluate incident circumstances to make sure the root cause is identified and remedied as well as confirm there is no further risk to information.

Post-incident analysis – Agencies shall thoroughly study the circumstances involved with the incident. A formal action plan aimed at precluding future incidents should be developed. The action plan must contain the following:

- Root cause applicability to other operations – assure that lessons learned are applied to other operational areas where the same or similar risks exist.
- Response evaluation – assess the response to the incident and the overall effectiveness of dealing with incident circumstances.
- Adjust response procedures – integrate improvements to agency incident management procedures.
- Training and awareness – educate appropriate parties on updated risk circumstances and updated incident management techniques.
- Report to CISO – The CISO will assess the action plan for appropriateness and applicability to other agency circumstances to improve the state’s overall security position.
- Assist other agencies – share experience with other agencies as applicable to help them avoid incidents and more effectively handle similar experiences.

Roles
Agency Executive Management
All Personnel
IOT Personnel

Responsibilities
All personnel are to be aware of the incident reporting process and report known or suspected security incidents to the State CISO. Agencies shall ensure employees have information necessary to identify and appropriately report security incidents to appropriate personnel. IOT shall provide guidance and support on appropriate responses to security incident(s).
Management Commitment
Management is responsible for ensuring their agency is aware of incident response processes and is able to meet the requirements written within this Standard.

Coordination Among Organizational Entities
Agencies shall coordinate with IOT on security incidents in accordance with this Standard.

Compliance
Unreported incidents may be subject to disciplinary action.

Exceptions
No exceptions.

Associated Documents
Incident Report Form