Kansas State University IT Security Post-Incident Report

Incident ID Number: YYYY-NNN

Incident Category(ies):

Classification(s) of Data Involved in the Incident (per the K-State Data Classification Schema)**:**

Incident Title:

Incident Manager (name, title, e-mail, phone)**:**

Incident Administrative Contact (name, title, e-mail, phone)**:**

Incident Departmental Contact (name, title, e-mail, phone)**:**

Date of Initial Suspicious/Malicious Activity:

Date Incident Reported:

Date Incident Fully Contained:

Post-Incident Review Session:
Date:
Participants:

Date Incident Response Completed:

Post-Incident Report Submitted by (name, title, e-mail, phone):

Date Post-Incident Report Submitted:

Incident Overview:
Provide a general overview of what happened, indicating how the security breach occurred and the scope of the incident (for example, who was affected, what systems were compromised, the dates of major milestones, etc.). Detailed information, like a timeline, may be added to the end of the report as appendices.

Incident Detection:
Briefly describe how the incident was first discovered (when, how, and by whom).

Incident Response:
Describe how the incident was contained (prevented from spreading and/or doing further damage) and eradicated (removed from infected hosts). Also describe recovery activities.

Incident Notification
If the incident involved the breach of, or suspected breach of personal identity information that requires notification, then describe how and when the affected people were notified. Include any public communications, like a press release.

Incident Follow-Up
Identify steps taken to prevent future incidents, lessons learned, and any other recommendations resulting from the incident and the post-incident review session.

A. Steps Taken to Prevent Future Incidents
i.

B. Lessons Learned
i. .

C. Other Recommendations
i.

Appendices
Attach any other relevant information about the incident that should be archived.