Kentucky Criminal Justice Information (CJI) Security Incident Response Plan

Agency Name:

Introduction

This Incident Handling and Response Plan establishes a comprehensive approach to managing security incidents involving Criminal Justice Information (CJI). This plan ensures compliance with the FBI CJIS Security Policy and Law Information Network of Kentucky (LINK) by outlining procedures for preparation, detection, analysis, containment, recovery, and reporting of incidents.

Incident Response Priorities *(Reference: IR-1: Incident Response Policy and Procedures)*
When an incident occurs, the following priorities must guide the response:

1. Protect Human Life and Safety: Ensure the safety of all personnel and the public.
2. Protect Classified Data: Prevent unauthorized access to or dissemination of classified data.
3. Protect Sensitive but Unclassified Data: Safeguard the confidentiality and integrity of sensitive but unclassified data.
4. Prevent Damage to Systems: Protect systems from damage, including loss or alteration of software, files, and hardware components.
5. Minimize Service Disruption: Reduce the impact on system availability and functionality.

Incident Reporting and Communication

Reporting Information Security Events *(Reference: IR-6: Incident Reporting)*
- Initial Reporting: All employees must report any security incident involving CJI immediately to their immediate supervisor, the Terminal Agency Coordinator (TAC), or the Local Agency Security Officer (LASO). This prompt reporting ensures that incidents are managed and resolved quickly.
- Escalation Procedures: Incidents that meet severity thresholds must be escalated to state security officials, including the Information Security Officer, Nehemiah J. Wilkinson at 502-782-9914.
- Notification Protocols: All incidents should be reported using designated communication channels, with email and secure messaging as primary methods for urgent communication.

Mobile Devices Incident Handling *(Reference: IR-5: Incident Monitoring)*
- Incident Reporting: Any loss, theft, or compromise of mobile devices containing CJI must be reported immediately to a supervisor, TAC, or agency management. Reports should include details such as device type, connectivity methods, and the device's security state at the time of the incident.
- Response Actions: Depending on the incident, actions may include remote wiping of data, device tracking, or notifying relevant authorities, especially if the device was lost or stolen outside the United States.

Detailed Incident Handling Procedures

Preparation *(Reference: IR-2: Incident Response Training)*
- Training: All personnel must receive role-based training on incident response procedures, with regular updates reflecting new threats and mitigation strategies. Training should include simulations and drills to prepare for real-world scenarios.
- Tools and Resources: Ensure the availability of necessary tools, including logging systems, forensic analysis software, and predefined communication protocols.

Detection and Analysis *(Reference: IR-4: Incident Handling)*
- Monitoring and Alerting: Implement continuous network and system monitoring to detect potential incidents in real-time. Utilize automated tools to generate alerts for unusual or suspicious activities. Ensure that all monitoring logs are securely stored and regularly reviewed.
- Incident Analysis: Conduct a detailed analysis of each incident to determine its scope, impact, and root cause. Document all findings comprehensively to aid in incident resolution and post-incident review.

Containment *(Reference: IR-4: Incident Handling)*
- Isolation Procedures: Upon detection of an incident, isolate affected systems to prevent the spread of the threat. This may involve disconnecting systems from the network, restricting user access, or shutting down specific services.
- Communication During Containment: Maintain clear, documented communication with all relevant parties, ensuring that the incident containment actions are understood and followed.

Eradication *(Reference: IR-4: Incident Handling)*
- Threat Removal: After containment, focus on eradicating the threat from all affected systems. This includes identifying and neutralizing malware, fixing vulnerabilities, and ensuring that no remnants of the threat remain.
- Verification: Conduct thorough testing to verify that all systems are free of threats before proceeding to recovery.

Recovery *(Reference: IR-4: Incident Handling)*
- System Restoration: Restore systems to full operational status once they have been secured. This may involve re-imaging devices, restoring data from backups, and performing thorough testing to confirm system functionality.
- User Notification and Guidance: Notify all users when systems are back online, providing any necessary instructions or warnings to prevent a recurrence.

Post-Incident Activities

Incident Reporting and Documentation *(Reference: IR-6: Incident Reporting)*
- Comprehensive Incident Reports: For every security incident, complete a detailed incident report. This report should include the nature of the incident, actions taken, and the resolution. Retain these reports in the agency's records and submit copies to the state Information Security Officer.
- Post-Incident Review and Analysis: Conduct a post-incident review to assess the response and identify areas for improvement. Update the incident response plan as needed based on lessons learned from the incident.

Continuous Training and Awareness *(Reference: IR-2: Incident Response Training)*
- Regular Refresher Training: Provide regular refresher training on incident response procedures, particularly after significant incidents or at predetermined intervals. Emphasize lessons learned and best practices.
- Policy and Plan Updates: Regularly review and update the Incident Response Plan to reflect changes in technology, threats, and FBI CJIS Security Policy requirements.

_____ _____

Signature of Agency Head Date

KENTUCKY STATE POLICE INFORMATION SECURITY OFFICER (ISO) SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

_____

LOCATION(S) OF INCIDENT: _____

INCIDENT DESCRIPTION: _____

_____

SYSTEM(S) AFFECTED: _____

_____

SYSTEM(S) AFFECTED (e.g., CAD, RMS, file server, etc.): _____

_____

METHOD OF DETECTION: _____

ACTIONS TAKEN/RESOLUTION: _____

_____

_____

Copies To:

Nehemiah J. Wilkinson
(KSP CJIS ISO)
1266 Louisville Road
Frankfort, KY 40601
502-330-4921
nehemiah.wilkinson@ky.gov

Security Incident Response Team Contact List
(Reference: IR-7: Incident Response Assistance)

[List all security team members, including Nehemiah J. Wilkinson, TAC, IT staff, and others as necessary.] ALL incidents should be reported to the KSP helpdesk so the ISO can be notified.

Name: Nehemiah J. Wilkinson	
Title: Information Security Officer (ISO) and CJIS Compliance Supervisor	
Work phone: 502-782-9914	Home phone: N/A
Mobile phone: 502-330-4921	Pager: N/A
Work email: nehemiah.wilkinson@ky.gov	

Name:	
Title:	
Work phone:	Home phone:
Mobile phone:	Pager:
Work email:	

Name:	
Title:	
Work phone:	Home phone:
Mobile phone:	Pager:
Work email:	

Name:	
Title:	
Work phone:	Home phone:
Mobile phone:	Pager:
Work email:	

External Contact List

[List all vendors (e.g., CAD vendor) and third-party organizations that may need to be contacted during a security incident.]

Product/Service/Relationship	
Organization Name:	
Street Address:	Phone Number: Fax Number:
Contact Person: Alternate Contact:	Email:
Comments:	

Product/Service/Relationship	
Organization Name:	
Street Address:	Phone Number: Fax Number:
Contact Person: Alternate Contact:	Email:
Comments:	

Product/Service/Relationship	
Organization Name:	
Street Address:	Phone Number: Fax Number:
Contact Person: Alternate Contact:	Email:
Comments:	