INFORMATION SECURITY OFFICER (ISO) SECURITY INCIDENT REPORT

AUTHORITY: MCL 28.215, MCL 28.162, and R 28.5201; **COMPLIANCE:** Mandatory; **PENALTY:** Loss of access to criminal justice information systems.

Agencies shall promptly report digital and physical incidents that significantly endanger the security or integrity of Criminal Justice Information (CJI) to the Michigan State Police Information Security Officer (ISO) in compliance with the Federal Bureau of Investigation (FBI) Criminal Justice Information Services (CJIS) Security Policy. If a question does NOT apply, enter "N/A" to signify not applicable.

Send Completed Hard Copy Form To:	**For Additional Information:**
Michigan State Police Criminal Justice Information Center Attn: Information Security Officer P.O. Box 30634 Lansing, MI 48909-0634	**FBI CJIS SECURITY POLICY** **Questions/Comments:** Phone: 517-284-3069

I. Agency Information

Point(s) of Contact (Full Name and Title)	Work Phone Number/Extension	Email Address	
Agency Name	Noncriminal Justice Agency ID	Criminal Justice Agency ORI	
Agency Address	City	State	ZIP Code
Date of Report	Date of Incident		

II. Incident Information

Incident Type
☐ Computer Security ☐ Digital Media ☐ Physical Media ☐ Mobile Device

Identify the time frame and the operational phase. (i.e., Was this a one-time occurrence or continuing? Could it occur anytime or do certain events trigger it?)

Location(s) of Incident

System(s) and/or Data Affected (e.g., Computer Aided Dispatch, Records Management System, File Server, Physical Media containing CJI)

Did access include any personally identifying information or CJI? ☐ Yes ☐ No	Is the hard drive encrypted? ☐ Yes ☐ No

Method of Detection/Discovery (e.g., via an audit trail, or accidental discovery)

Describe the incident. Why did this incident happen? What allowed this incident to occur? Were there policies in place which may be applicable to this incident? Should there be controls in place which may help to prevent this type of incident from reoccurring?

Actions Taken/Resolution

What are the vulnerabilities and impacts associated with this incident? Describe what you believe are the vulnerabilities and impacts to other information systems/criminal justice information as a result of this incident. Provide a description/list as to who you believe is affected or vulnerable to a similar incident.

III. Additional or Enhanced Incident Response for Mobile Device Operating Scenarios

Did the mobile device contain or access CJI?
☐ Yes ☐ No

Describe the loss of mobile device control. (i.e., was the mobile device known to be locked or unlocked and the duration of the loss)

Was there a total loss of the mobile device? (i.e., the mobile device has not been recovered)

Was criminal justice information stored on the mobile device? Was the mobile device used to access criminal justice information services or systems? Was the mobile device enrolled in Mobile Device Management? Was the mobile device remote locked or wiped? Was your agency able to determine the last known location of the mobile device? Was your agency able to recover the mobile device?

Did the mobile device loss of control, total loss, or compromise occur outside the United States?