Resources for Developing Security Incident Related Procedures
Local Criminal Justice Agency Version

The security risk of both accidental and malicious attacks against government and private agencies remains persistent in both physical and logical environments. To ensure protection of criminal justice information, agencies shall: (i) establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.
(*FBI CJIS Security Policy*, Version 5.6, June 2017, Policy Area 3: Incident Response, pp 24-26)

Revisions are published on an annual basis and agencies are responsible for complying with the requirements in the most current version.

FBI CJIS Security Policy Resource Center
https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

- Section 3.2.9 Local Agency Security Officer
- Policy Area 3: Incident Response
    - Section 5.3.1 Reporting Security Events
    - Section 5.3.2.1 Incident Handling
    - Section 5.3.2.2 Collection of Evidence
    - Section 5.3.4 Incident Monitoring
- Policy Area 13: Mobile Devices
    - Section 5.13.5 Incident Response [for mobile device operating scenarios]

- Security Control Mapping of CJIS Security Policy (posted on Resource Center website)
    - The CJIS Security Policy is mapped to the National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Assessing Security and Privacy Controls for Federal Information Systems and Organizations

SANS Institute, Reading Room
https://www.sans.org/reading-room/whitepapers/incident

- Incident Handler’s Handbook
- Incident Handling for SMEs (Small to Medium Enterprises)

National Institute of Standards and Technology

- Computer Security Incident Handling Guide,
  Special Publication 800-61 Revision 2
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- Guide to Malware Incident Prevention and Handling for Desktops and Laptops,
  Special Publication 800-83 Revision 1
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf

Michigan Cyber Security
http://www.michigan.gov/cybersecurity

- Michigan Cyber Disruption Response Plan

Local Agency Security Officer (LASO) Appointment Form
http://www.michigan.gov/documents/msp/CJIS-007_331565_7.pdf

Michigan State Police Information Security Officer Security Incident Reporting Form
http://www.michigan.gov/documents/msp/cjis-016_Final_Rev_11_1_16_540177_7.doc

Example: The Michigan State Police (MSP) utilizes agency specific security awareness training, local policies and procedures, Official Correspondence, and Official Orders. The MSP has management control over state IT personnel and also utilizes their policies, procedures, and processes related to incident response in support of our agency. The State of Michigan has a Cyber Disruption Response Plan.

Note: A sample policy/procedure will not be created; documentation needs to be specific to each agency.

Revised June 13, 2017