Keller PD NETCOM Incident Handling and Response Plan Date: 09/01/2014

TLETS Security Incident Response Plan - There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile. The following establishes an operational incident handling procedure for Keller PD NETCOM CJIS, TCIC/NCIC, and TLETS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate NETCOM personnel, TCIC agency officials and/or authorities. David Hanks- LASO is the department's point-of-contact for security-related issues and will ensure the incident response reporting procedures are initiated at the local level.

As the criminal justice community becomes more dependent on global network technology, the reasons for the attacks can be accidental or malicious. The effects of these intrusions can range from embarrassment, to causing the inability to function, to the loss of human life. Because incidents can have many possible consequences that range from slight to catastrophic, priorities must be considered when evaluating and processing incidents. The following five priorities should be evaluated when an incident occurs:

Priority 1 - Protect human life and people's safety.

Priority 2 - Protect classified data.

Priority 3 - Protect Sensitive But Unclassified data.

Priority 4 - Prevent damage to systems (e.g., loss or alteration of system software and files,

damage to disk drives, etc.).

Priority 5 - Minimize disruption of computing resources.

Reporting Information Security Events - The department will promptly report incident information to appropriate authorities. Information security events and weaknesses associated with information systems shall be communicated in a manner allowing timely corrective action to be taken. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents. All Dispatchers will be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of agency assets and are required to report any information security events and weaknesses as quickly as possible to the Support Services Supervisor.

Reporting Procedures for Suspected and Actual Security Breaches:

- If you become aware of any policy violation or suspect that your password may have been used by someone else, first, change your password and, then, report the violation immediately to the Support Services Supervisor.

Virus Reporting Procedures and Collection of Security Incident Information:

- Upon identifying a problem, disconnect the TLETS coax cable from the TLETS Hughes modem.
- Notify Travis Trevino, David Hanks and Keith Macedo and the appropriate Chain-of-Command.
- Notify Keith Macedo Information Technology Security Administrator.
- Notify the TLETS Operations Intelligence Center (OIC) at 1-888-DPS-OIC0 (1-888-377-6420)
- Identify who will run your traffic in the meantime while you fix the problem.
- Notify Member Departments Southlake and Colleyville of situation if required.
- Compile information for completing an Information Security Response Form
    - Suspected cause for incident (Name, virus, etc.)
    - Was Antivirus software running at the time of infection?
    - How and when the problem was first identified?
    - Has Local IT staff been notified/are they involved?
    - Number of workstations infected?
    - Any other equipment infected?
    - Action plan for removal.
    - Will infected workstations be re-imaged before reconnection?
    - When was the last update of signature files?
    - When was the last operating system update?
    - Was any CJIS data or personnel identification information compromised?
- The TLETS system will remain disconnected from TLETS until Keith Macedo and David Hanks can guarantee your systems are free from virus infection.
- Once free from infection and given clearance by the CJIS Security Group on-call person, the system can be reconnected to TLETS and NLETS.

TLETS SECURITY INCIDENT RESPONSE FORM

REPORTING FORM

DATE OF REPORT: DATE OF INCIDENT:

REPORTING PERSON:

PHONE/EXT/E-MAIL:

LOCATION(S) OF INCIDENT:

SYSTEM(S) AFFECTED:

METHOD OF DETECTION:

NATURE OF INCIDENT:

INCIDENT DESCRIPTION:

ACTIONS TAKEN/RESOLUTION:

PERSONS NOTIFIED: