CHAPTER # 26 POLICE INFORMATION	POLICY # 26.6 SECURITY INCIDENT RESPONSE PLAN
This policy is for internal use only and does not enlarge an employee's civil liability in any way. The policy should not be construed as creating a higher duty of care, in an evidentiary sense, with respect to third party civil claims against employees. A violation of this policy, if proven, can only form the basis of a complaint by this department for non-judicial administrative action in accordance with the laws governing employee discipline.	
Date Implemented: 11/18/2022	Review Date:

Kentucky 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 the Indian Hills Police Department's CJIS, LINK/NCIC, and NLETS information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate Indian Hills Police Department personnel, Kentucky agency officials and/or authorities. The Indian Hills Police Department's Chief of Police 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/alteration of software and files, damage to drives, etc.).

Priority 5 - Minimize disruption of computing resources.

Reporting Information Security Events

The Indian Hills Police 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 Indian Hills Police Department will use email to

expedite the reporting of security incidents. All Dispatchers for Criminal Justice Agencies and all authorized personnel for Non-Criminal Justice Agencies will be made aware of the procedures for reporting the different types of events 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 immediate 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 Chief of Police.

Reporting Information on Mobile Devices

Mobile devices present unique security challenges from suspected loss of device control, device lost or stolen (including outside U.S.) or device becomes compromised. Both the device type and connectivity methods installed and configured on the device will impact the overall risk scenario associated with the device. Each device type and policy defined is based on the inherent risk associated to such device.

Laptop devices

The laptop device type includes mobile devices in a larger format that are transported either in a vehicle mount or a carrying case and include a monitor with attached keyboard. This includes traditional laptop computers and 'tablet' type full featured computers running a traditional full featured operating system but without an attached keyboard. The main defining factor is the use of a full featured operating system and a form factor too large to be carried in a pocket.

Tablet devices

The tablet device type includes larger format devices transported via vehicle mount or portfolio sized carry case that typically consist of a touch screen without attached keyboard. These devices utilize a limited feature operating system (e.g., Apple iOS, Google Android, Windows mobile) and have limited operating feature sets. Operating systems designed specifically for the mobile environment where battery life and power efficiency are primary design drivers.

Pocket devices/Handheld devices

The pocket/handheld device type is technically similar or identical to the tablet category and is primarily differentiated by device form factor. Pocket/handheld devices are characterized as having a limited functionality operating system and a small form factor intended for carry in a pocket or 'holster' attached to the body. The bulk of this category will be cellular 'smartphones' with integrated cellular data connectivity.

Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface. This includes rooting, jail breaking or malicious application installation on the device during a loss of device control scenario or inappropriate user action in the installation of applications to the device (compromise can occur from intentional actions or accidental user actions). Knowing the device lock state, duration of loss, total loss of CJI stored can help determine any capabilities for remote wiping or device tracking. Triggers for this incident handling process may be driven from either user notification or electronic detection of device tampering from an audit or MDM compliance check.

Reporting Procedures for Mobile Devices

Personnel shall report immediately any incident involving loss of device control, device lost or stolen (including outside U.S.) or device becoming compromised to the Chief of Police so steps can be taken to resolve the situation and/or mitigate the risk. Formal event reporting and escalation procedures shall be in place. Wherever feasible, the department will use email to expedite the reporting of security incidents.

Virus Reporting Procedures and Collection of Security Incident Information

- Upon identifying problem, if applicable, disconnect the device.
- Notify the Chief of Police.
- Notify Erin Oliver Kentucky's Information Security Officer at 502-382-6780.
- Identify who will run agency traffic in the meantime while the problem is being resolved.
- Notify Contractor(s) 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 and are implementing a resolution?
- Number of workstations, laptops, tablets or cell devices infected.
- Any other equipment infected?
- Action plan for removal.
- Will infected devices be re-imaged or wiped before reconnection?
- When was the last update of anti-virus signature files?
- When was the last operating system update?
- Was any CJIS data or personal identification information compromised?
- The system will remain disconnected from LINK/NCIC until it can guarantee your systems are free from virus infection.
- Once free from infection and given clearance, the system can be reconnected.

KENTUCKY SECURITY INCIDENT RESPONSE FORM

DATE OF REPORT: _____/_____/_____   DATE OF INCIDENT: _____/_____/_____

REPORTING PERSON: _____

PHONE/EXT/E-MAIL: _____

LOCATION(S) OF INCIDENT: _____

SYSTEM(S) AFFECTED: _____
_____

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

METHOD OF DETECTION: _____
_____

NATURE OF INCIDENT: _____
_____

INCIDENT DESCRIPTION: _____
_____
_____

ACTIONS TAKEN/RESOLUTION: _____
_____
_____

PERSONS NOTIFIED:

Security Incident Response Team Contact List

Name: Kelly Spratt	
Title: Chief of Police	
Work phone: 502.537.0718	Home phone:
Mobile phone: 502.338.4788	Pager:
Work email: spratt@ihpd.org	
Alternate email:	
Home address:	

Name: Thomas Coin	
Title: Lieutenant	
Work phone: 502.537.0632	Home phone:
Mobile phone:502.640.8058	Pager:
Work email: coin@ihpd.org	
Alternate email:	
Home address:	

External Contact List

Product/Service/Relationship: Communications Center	
Organization Name: Jefferson County Sheriff's Office	
Street Address: 531 Court Place	
City/State/Zip: Louisville, KY 40202	
Contact Person: Jennifer Cravens Alternate Contact:	Phone Number: 502.574.8109 24 Hour Number: 502.574.5471 FAX Number: 502.574.6909 Email: jcravens@jcsoky.org
Comments:	

Product/Service/Relationship:	
Organization Name: Kentucky State Police	
Street Address:	
City/State/Zip:	
Contact Person: Erin Oliver Alternate Contact:	Phone Number: 502.382.6780 24 Hour Number: FAX Number: Email: erin.oliver@ky.gov
Comments:	