CJIS/CHRI Security Incident Reporting

Policy Statement

To ensure protection of Criminal Justiec Information (CJI), the Whatcom County Sheriff's Office (WCSO) will establish operation incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities to track, document and report incidents security incidents to appropriate WCSO staff and/or WSP/ACCESS.

Persons Affected

All Sheriff's Office personnel.

Definitions

CHRI – Criminal History Record Information (Rapsheet/III)

CJI – Criminal Justice Information

Security Incident - a change in the everyday operations of a network or information technology service indicating that a security policy may have been violated or a security safeguard may have failed.

Reporting Security Incidents

The WCSO will promptly report incident information to the ACCESS Information Security Officer (ISO) [redacted] . The WCSO staff will use the *FBI Security Incident Reporting Form* in PowerDMS or [redacted].

Security events, including identified weaknesses associated with the event, 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 WCSO shall employ automated mechanisms to assist in the reporting of security incidents. All employees, contractors and third party users shall be made aware of the procedures for reporting the different types of events and weakness that might have an impact on the security of County assets. All WCSO employees are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

Management of Security Incidents

A consistent and effective approach shall be applied to the management of security incidents. Responsibilities and procedures shall be in place to handle security events and weaknesses effectively once they have been reported.

Incident Handling

The WCSO shall implement an incident handling capability for security incidents that includes; preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the WCSO shall employ automated mechanisms to support the incident handling process.

Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. The WCSO will incorporate lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly.

Collection of Evidence

Where a follow-up action against a person or the WCSO after an information security incident involves legal action (either civil or criminal), evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

Incident Response – Mobile Devices

In addition to the requirements in Incident Response, the WCSO shall develop additional or enhanced incident reporting and handling procedures to address mobile device operating scenarios. 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.

Special reporting procedures for mobile devices shall apply in any of the following situations:

1. Loss of device control. For example:
    a. Device known to be locked, minimal duration of loss.
    b. Device lock state unknown, minimal duration of loss.
    c. Device lock state unknown, extended duration of loss.
    d. Device known to be unlocked, more than momentary duration of loss
2. Total loss of device.
3. Device compromise.
4. Device loss or compromise outside the US.