



# Administrative Policy and Procedure

## City of Prosser, Washington

<b>SUBJECT: ACCESS Security Incident Reporting</b>		
	Policy No. IT.003	Pages: 2
Effective Date: October 22, 2018		
Developed By: Rachel Shaw, City Clerk	Department Head Approval: Rachel Shaw, City Clerk	City Administrator Approval:

### OVERVIEW

#### 1. INCIDENT RESPONSE

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 (CJI), the City of Prosser is required to establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities; track, document, and report incidents to appropriate agency officials and/or authorities.

#### 2. REPORTING SECURITY EVENTS

The City of Prosser Police Department shall promptly report incident information to the ACCESS Information Security Officer (ISO) by email to [ACCESS@wsp.wa.gov](mailto:ACCESS@wsp.wa.gov) using the FBI Security Incident Reporting Form available on the ACCESS webpage: [http://www.wsp.wa.gov/secured/access/docs/access\\_cjis\\_security\\_incident\\_report.pdf](http://www.wsp.wa.gov/secured/access/docs/access_cjis_security_incident_report.pdf).

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 and are outlined in IT Policy 001. Wherever feasible, the agency 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 event and weakness that might have an impact on the security of agency assets and are required to report any security events and weaknesses as quickly as possible to the designated point of contact.

#### 3. 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 and are outlined in IT Policy 001.

**4. INCIDENT HANDLING**

The City shall implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the City 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 City should incorporate the lessons learned from ongoing incident handling activities into the incident response procedures and implement the procedures accordingly as outlined in IT Policy 001..

**5. COLLECTION OF EVIDENCE**

Where a follow-up action against a person or agency 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).

**6. INCIDENT RESPONSE – MOBILE DEVICES**

In addition to the requirements in Incident Response, agencies 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:

- 6.1. 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
- 6.2. Total loss of device
- 6.3. Device compromise
- 6.4. Device loss or compromise outside the United States