<INSERT AGENCY NAME(S)>

CJIS/CHRI Data Breach Reporting

|  |
| --- |
| *The purpose of this template is to assist your agency in creating its own procedures. These are the minimum topics that must be covered:**\*\*\*\*\*This document can cover multiple agencies supported by the same IT team\*\*\*\*\**1. *The items below in red must be specific and reflect your agency’s current practices.*
2. *Remove any items that are not applicable to your agency.*
3. *Formalize with the date and your agency name.*
4. *Remove the red box once the procedure is updated and completed.*

*If your procedure does not reflect the actual practice at your agency, then you will be found out of compliance.**ACCESS Section revised March 2021* |

**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), agencies shall:

1. Establish operational incident handling procedures that include adequate preparation, detection, analysis, containment, recovery, and user response activities;
2. Track, document, and report incidents to appropriate agency officials and/or authorities.

**Reporting Security Events**

<Insert Agency Name> shall promptly report incident information to the ACCESS Information Security Officer (ISO) by email to ACCESS@wsp.wa.gov using the *FBI Security Incident Reporting Form* available on the ACCESS webpage: <http://www.wsp.wa.gov/_secured/access/docs/cjis_security_incident_report_form.pdf> to any authorities appropriate to the local agency.

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 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 events 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.

**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 agency shall implement an incident handling capability for security incidents that includes; preparation, detection and analysis, containment, eradication, and recovery. Wherever feasible, the agency 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 agency should incorporate the 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 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).

**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:

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 United States