STATE OF ALASKA DEPARTMENT OF CORRECTIONS POLICIES & PROCEDURES	SECTION: **Administration**		PAGE: Page **1** of **4**
	CHAPTER: **650**	NUMBER: **650.08**	P&P TYPE: **Public**
	TITLE: **CJIS Incident Reporting / Response**		
	APPROVED BY: **Nancy A. Dahlstrom, Commissioner**		DATE: **01/28/22**
ATTACHMENTS / FORMS: **A. CJIS Incident Report**	AUTHORITY / REFERENCES: **22 AAC 05.155** **AS 33.05.010** **AS 33.16.180** **AS 33.30.011** **AS 33.30.021** **AS 44.28.030** **DOC P&P 202.01** **DOC P&P 202.15** **FBI CJIS Security Policy** **DPS CJIS Systems Agency (CSA) Policy** **SOA/OIT Policy 5.8.1 ISP-151: Incident Response** **SOA/OIT Policy 5.8.2 ISP-152: Incident Reporting**		

DISCUSSION:

There have been an increased number of accidental and / or malicious digital attacks against both government and private agencies, regardless of whether the systems are high, or low, profile. Precautions regarding the security of physical records also need to be considered. The effects of these intrusions can range from embarrassment to a complete inability to function, to the loss of human life. As the criminal justice community becomes more dependent on global network technology, it is important to have in place a method of response, and reporting, of such occurrences. The following establishes an operational information security incident handling procedure for the Department of Corrections (DOC).

POLICY:

I. It is the policy of the Department of Corrections (DOC) to have in place procedures that ensure an effective and appropriate response to all security events, and incidents, related to the confidentiality, integrity, and availability of DOC criminal justice information services (CJIS) and criminal justice information (CJI), and, that suspected events are classified as an incident and appropriately investigated.

II. It is the policy of the Department to have in place procedures that establish the proper reporting of all security events and incidents.

APPLICATION:

This policy and procedure will apply to all Department employees, contractors, consultants, temporary staff, and any other related entity. This policy and procedure will apply to all equipment that is owned or leased by DOC and/or is connected to the DOC network, as well as all CJI; in digital or physical format.

DEFINITIONS:

For additional definitions of key words or phrases used in this policy, please refer to the Definitions section of DOC P&P 651.01 (Criminal Justice Information Access).

Findings:
Conclusions and determinations reached as a result of a CJIS security incident investigation.

PROCEDURES:

I. Incident Identification and Priority:

A. Initial Identification of an Incident:

1. Digital incidents may include:

a. Unauthorized access to information system and / or device;
b. Inappropriate use (business need);
c. Lost media; and
d. Intrusion via malware.

2. Physical incidents may include:

a. Unauthorized access to physical file and / or printed materials;
b. Inappropriate use (business need);
c. Lost files and / or printed materials;
d. Destruction (accidental or malicious); and
e. Openly discussing CJI / Personally Identifiable Information (PII) in the vicinity of others who are not cleared to receive the information.

B. CJIS security incidents should be thoroughly investigated by a supervisor, TAC, and/or CJIS Unit. The investigation process of the security incident shall include the gathering of evidence (when applicable). Where possible the supervisor, TAC, and/or CJIS Unit's investigation should answer questions such as (but not limited to):

1. What happened?

2. When did it happen?

3. Where did it happen?

4. How did it happen?

5. Who was involved?

6. Was there any malicious intent?

7. What safeguards failed? (if any)

8. What are the repercussions? (if any)

9. What could be done to prevent future incidents?

Evidence gathered for security incident investigations may include (but is not limited to): interviews conducted with employees, written statements by staff, hard copy print outs, system or security logs gathered by OIT and/or DOC CJIS, security video footage, any physical or digital information. All evidence will be sent to CJIS Unit for review and consideration leading to any potential findings.

II. Incident Reporting:

A. A CJIS Incident Report Form (Attachment A) shall be filled out at the location of the incident, within two (2) hours of the occurrence.

B. The CJIS Incident Report Form shall be reviewed by a supervisor and forwarded to appropriate Terminal Agency Coordinator (TAC).

C. The TAC shall forward the incident report (via scan and e-mail) to the DOC CJIS Unit (doc.cjis@alaska.gov), where upon receipt, a tracking identification number shall be assigned.

D. All incident reports will be submitted to the DOC CJIS Unit within 24 hours or by the next business day.

III. Incident Response:
The DOC CJIS Unit will investigate the incident based on the following:

A. Findings will be established.
1. Identify if an incident has occurred.

B. In the event of an incident, severity shall be determined.
1. **HIGH:** Exposure (or possible exposure) of criminal justice information (CJI), personally identifiable information (PII), protected health information (PHI), Controlled Unclassified Information (CUI), classified information, or other data that could lead to critical losses if disclosed or corrupted.

2. **MEDIUM:** Exposure (or possible exposure) of confidential information that if lost or disclosed could result in a significant loss to the department.

3. **LOW:** Limited or no exposure of confidential information (i.e., Misuse of system, no business reason).

**Previous incidents may factor into severity level.*

C. Required action(s) will be forwarded to the TAC and the appropriate management staff. Required actions based on incident severity:
   1. Suspension of accounts/restrictions to areas.
   2. Notice to location supervisor and TAC.

D. Reinstatement of CJIS Clearance
   1. Review and sign appropriate policies/documents.
   2. Remedial security awareness training.
   3. All medium and high severity incidents shall be forwarded to the appropriate Director's office for review.

E. Update CSA-ISO of finding(s), action(s), and incident status.

IV. Incident Resolution:
Upon completion of an incident response, the CJIS Unit, location supervisor, TAC will:

A. Confirm that any required actions are completed.;

B. Confirm that any additional findings of non-compliance/security issues are resolved.

C. Complete a debrief of the security incident with all parties involved and consider implementation of any additional recommendations for security improvements.

D. Close out the incident tracking ticket.