CITY OF ANDERSON POLICE DEPARTMENT
Anderson, South Carolina

DIRECTIVE TYPE General Order	EFFECTIVE DATE July 15, 2019	NUMBER 2419
SUBJECT CJI INCIDENT REPSONSE POLICY	REVISED	
REFERENCE All Others	AMENDS/SUPERSEDES All Others	
DISTRIBUTION All Personnel	RE-EVALUATION DATE Annual	Number of Pages: 2

Security Incident Response

1. Overview

A security incident response addresses how the City of Anderson Police Department will handle a confirmed security incident that resulted in a compromise of criminal justice information (CJI), whether the breach, theft, intrusion, or other such violation was physical (e.g., paper files, copies of fingerprint cards, etc.) or logical (i.e., digital). Notification to the South Carolina Law Enforcement Division (SLED Criminal Justice Information Security Officer (ISO) is required if the incident involved CJI.

2. Purpose

The purpose of this policy is to outline the steps City of Anderson Police Department will take for a confirmed security incident that involves CJI.

3. Scope

This policy applies to employees, contractors, consultants, temporary staff, and other workers at City of Anderson Police Department, who work with or have access to State and/or FBI criminal justice information (CJI). This policy applies to all equipment that is owned or leased by City of Anderson Police Department.

4. Policy

Whoever discovers the incident shall immediately contact the Chief of Police or IT. S/he shall note, in incident report and APD Form as much detail as possible, what was occurring that lead up to the discovery of the incident.

1. The Chief of Police or his designee shall conduct an investigation to determine what caused the purported incident.
2. If a security incident is declared, City of Anderson Police Department will take the following steps:
3. For an incident involving physical breaches (building break-ins, stolen items, etc.), City of Anderson Police Department shall do the following:
Officer conducting investigations shall be guided by the following steps.

a) Observe and record conditions, events, and remarks at incident scene.
b) Locate and identify witnesses.
c) Maintain integrity of the crime scene and protect all evidence.
d) Interview complainant and all witnesses.
e) Interrogate the suspect.
f) Arrange for collection of evidence.
g) Arrest the offender.
h) Report the incident fully and fairly.
i) Notify specialty investigators if applicable.

4. For an incident involving logical breaches (hacking, social engineering, ransomware, etc.), City of Anderson Police Department shall do the following:

a) Move quickly to secure all systems.
b) Identify the cause of the breach and resolve all vulnerabilities that led to it.
c) Try to determine the extent of the breach and what data was exposed.
d) Contact SLED and report our findings.
e) Once systems are secure and issues resolved, document the incident.
f) Formulate steps to prevent this from happening again.

5. Within twenty-four (24) hours of a declared security incident, the SLED Governance Risk and Compliance (GRC) unit shall be notified at laso@sled.sc.gov or 803-422-3297.
6. After the incident is resolved, City of Anderson Police Department will confer with all parties involved in the security incident response and develop a "Lessons Learned" report which will detail the incident and response actions, as well as how City of Anderson Police Department will reassess existing policies and procedures to reduce the likelihood of a repeat security incident.

By order of:

J Stewart

Jim Stewart, Chief of Police

7-16-19

Date