Charleston County Sheriff's Office
Policy and Procedures Manual

Sheriff Carl Ritchie

5-18
INFORMATION TECHNOLOGY INCIDENT RESPONSE (SECURITY INCIDENT/BREACH)

☐ NEW
☒ REVISED
☒ REVIEWED

ACA Standards Reference:
CALEA Standards Reference:
NCCHC Standards Reference:
SCLEA Standards Reference:
SC Minimum Standards:

This policy dated 1/28/2025 replaces prior policies cited above and supersedes all previously issued directives.

I. Purpose:

The purpose of this policy is to outline the steps that the Charleston County Sheriff's Office will take for a confirmed information technology breach or security incident that involves CJI and/or systems used to process, store, or transmit CJI.

II. Policy:

A breach or security incident response addresses how the Charleston County Sheriff's Office 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) Information Security Officer (ISO) is required if the incident involved CJI.

III. Definitions:

A. For purposes of this procedure, the word "deputy" applies to all agency employees with a certification classification of Class I, Class II, or Class III, as defined by the South Carolina Criminal Justice Academy.

The following terms are used interchangeably; however, they carry guidance to specific employees based on usage of the term.

1. Deputy, deputy sheriff, detention deputy, sworn employee, uniformed sworn employee, sworn administrative employee, and

2. civilian, non-sworn employee.

B. *Employee:* When used without further clarification, the term employee is inclusive of all agency members (sworn and non-sworn).

IV. Procedure:

A. Discovery of an Information Technology breach or security incident and response:

1. Whoever discovers the incident shall immediately contact the on-call Information Technology personnel. They shall note, in as much detail as possible, what was occurring that led up to the discovery of the incident.

a. The Information Technology System Manager shall then conduct an investigation to determine what caused the purported incident.

b. If a security incident is declared, the Charleston County Sheriff's Office will activate and follow procedures located in the Charleston County Sheriff's Office IT Disaster Recovery and Incident Reporting Plan.

c. For an incident involving physical breaches (building break-ins, stolen items, etc.), the Charleston County Sheriff's Office will activate and follow procedures located in the Charleston County Sheriff's Office IT Disaster Recovery and Incident Reporting Plan.

d. For an incident involving logical breaches (hacking, social engineering, ransomware, etc.), the Charleston County Sheriff's Office will activate and follow procedures located in the Charleston County Sheriff's Office IT Disaster Recovery and Incident Reporting Plan.

e. Within twenty-four (24) hours of a declared security incident, SLED shall be notified at cyber@sled.sc.gov or 803-896-8081.

f. After the incident is resolved, Charleston County Sheriffs Office 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 [agency name] will reassess existing policies and procedures to reduce the likelihood of a repeat security incident.

B. Compliance:

Employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to IT resources, and other actions as well as both civil and criminal penalties.