Charleston County Sheriff's Office
Policy and Procedures Manual

Sheriff Carl Ritchie

5-16
SYSTEM AND INFORMATION INTEGRITY

☒ 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:

To ensure that Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

II. Policy:

This policy is applicable to all departments and users of the Charleston County Sheriff's Office resources and assets.

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. Flaw Remediation:

The Charleston County Sheriff's Office will:

1. Identify, report, and correct information system flaws.

2. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

3. Install security-relevant software and firmware updates within the number of days listed after the release of the updates:

a. Critical – fifteen (15) days
b. High – thirty (30) days

c. Medium – sixty (60) days

d. Low – ninety (90) days

4. Incorporate flaw remediation into the configuration management process.

5. Perform vulnerability scanning at least quarterly or following any security incidents involving CJI or systems used to process, store, or transmit CJI.

B. Malicious Code Protection:

The Charleston County Sheriff's Office will:

1. Employ signature based malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

2. Automatically update malicious code protection mechanisms whenever new releases are available in accordance with configuration management policy and procedures.

3. Configure malicious code protection mechanisms to:

a. Perform periodic scans of the information system at least daily and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with the security policy; and

b. block or quarantine malicious code, take mitigating action(s), and when necessary, implement incident response procedures; and send alert to system/network administrators and/or organizational personnel with information security responsibilities in response to malicious code detection.

4. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

C. Information System Monitoring:

The Charleston County Sheriff's Office will:

1. Monitor the information system to detect:

   a. Attacks and indicators of potential attacks; and

   b. unauthorized local, network, and remote connections.

2. Identify unauthorized use of the information system through defined techniques and methods.

3. Deploy monitoring devices strategically within the information system to collect agency determined essential information and at ad hoc locations within the system to track specific types of transactions of interest to the entity.

4. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

5. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.

6. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable state and federal laws, directives, policies, or regulations.

7. Provide information system monitoring information to authorized personnel or business units as needed.

D. System-Generated Alerts:

The Charleston County Sheriff's Office will ensure that:

1. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized

personnel or business units that shall take appropriate action on the alert(s).

2. Alerts can be transmitted telephonically, electronic mail messages, or by text messaging as required. Personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

E. Security Alerts, Advisories, and Directives:

The Charleston County Sheriff's Office will:

1. Receive information system security alerts, advisories, and directives from external sources on an ongoing basis.

2. Generate internal security alerts, advisories, and directives as deemed necessary.

3. Disseminate security alerts, advisories, and directives to: organizational personnel implementing, operating, maintaining, and using the system; and

4. Implement security directives in accordance with established time frames or notify the issuing organization of the degree of noncompliance.

F. Software, Firmware, and Information Integrity:

The Charleston County Sheriff's Office will:

1. Employ integrity verification tools to detect unauthorized changes to software, firmware, and information systems that contain or process CJI; and

2. Take the following actions when unauthorized changes to the software, firmware, and information are detected: notify organizational personnel responsible for software, firmware, and/or information integrity and implement incident response procedures as appropriate.

3. Perform an integrity check of software, firmware, and information systems that contain or process CJI at system startup, restart, shutdown, and abort or security relevant events at least weekly or in an automated fashion.

4. Incorporate the detection of the following unauthorized changes into the organizational incident response capability: unauthorized changes to established configuration setting or the unauthorized elevation of system privileges.

G. Spam Protection:

The Charleston County Sheriff's Office will:

1. Employ spam protection mechanisms at information system entry and exit points to detect and act on unsolicited messages.

2. Update spam protection mechanisms when new releases are available in accordance with the configuration management policy and procedures.

3. Automatically update spam protection mechanisms at least daily.

H. Information Input Validation:

The Charleston County Sheriff's Office will check the validity of the following information inputs: all inputs to web/application servers, database servers, and any system or application input that might receive or process CJI.

I. Error Handling:

The Charleston County Sheriff's Office will ensure the information system:

1. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited; and

2. Reveals error messages only to organizational personnel with information security responsibilities.

J. Information Management and Retention:

The Charleston County Sheriff's Office will:

1. Manage and retain information within the system and information output from the system in accordance with applicable laws, executive orders, directives, regulations, policies, standards, guidelines, and operational requirements.

2. Limit personally identifiable information being processed in the information life cycle to the minimum PII necessary to achieve the purpose for which it is collected.

3. Use the following techniques to minimize the use of personally identifiable information for research, testing, or training: data obfuscation, randomization, anonymization, or use of synthetic data.

4. Use the following techniques to dispose of, destroy, or erase information following the retention period: overwrite technology at least three times, degauss digital media, or destroy.

K. Memory Protection:

The Charleston County Sheriff's Office will implement the following controls to protect the system memory from unauthorized code execution: data execution prevention and address space layout randomization.

L. 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.