**MYRTLE BEACH POLICE DEPARTMENT**

**ADMINISTRATION REGULATIONS AND OPERATING PROCEDURES**

| | |
|---|---|
| **Subject: Computer Security Incident** | **Number: 133-A** |
| **Effective Date:** January 10, 2019 | **Revised Date:** October 24, 2023 |
| **Rescinds:** 133 – Computer Security Incident | **Dated:** 01-10-19 |

Approved By:

## I. Purpose:

Improve the security of Myrtle Beach Police Department's information infrastructure, minimize the threat of damage resulting from an incident and promote the prevention of such incidents in the future.

## II. Definition:

1. *Computer Security Incident*: Any adverse event that threatens the confidentiality, integrity, or availability Department information assets, information systems, and the networks that deliver the information. Any violation of computer security policies, acceptable use policies, or standard computer security practices is an incident. Adverse events may include, denial-of-service attacks, loss of accountability, or damage to any part of the system. Examples include the insertion of malicious code (e.g. viruses, Trojan horses, or backdoors), unauthorized scans or probes, successful and unsuccessful intrusions, and insider attacks.

## III. Objectives:

a. Better communication/coordination between the teams involved to prevent a disjointed, non-cohesive response.

b. Provide rapid detection and containment of incidents and minimize disruption to business and network operations.

c. Establish controls for proper retrieval and handling of evidence and protect privacy rights established by law and policy.

d. Provide accurate reports and useful recommendations to participating teams and management.

e. Promote rapid detection and/or prevention of such incidents in the future via lessons learned discussions.

## IV. Roles and Responsibilities:

Within this section, the roles and responsibilities for all employees, Information Systems, Local Agency Security Officer, and Supporting Groups are defined.

A. Everyone

1) Report the suspected incident to the Information Systems, Local Agency Security Officer or your supervisor.

B. Information Systems (Police Department IT personnel)

1) Determines the nature and scope of the incident.
2) Notify affected departments, third parties, vendors, etc. of the situation and determine plan of action.
3) Escalates to executive management as appropriate.
4) Contacts auxiliary departments as appropriate.
5) Monitors progress of the investigation.
6) Ensures evidence gathering, chain of custody, and preservation is appropriate.
7) Prepares a written summary of the incident and corrective action taken.

C. Local Agency Security Officer

1) Notify the CSA at SLED within 24 hours of a declared incident via cyber@sled.sc.gov.
2) Continue to advise the CSA of significant or suspicious events that may be related.
3) Provide all related notes or logs for the integration into incident report.

D. Network Operations (Police Department IT personnel)

1) Initiate packet activity logging on the switch port (Should log to the appropriate zone syslog server). Notify the ISA and Information Security of the physical location of the affected device or system.
2) Take action necessary to block traffic from suspected intruder.
3) Continue to advise the Incident Handling Team of significant or suspicious events that may be related.
4) Forward all related notes or logs to the Incident Handling Team for end review.

E. Information Security Administrators (Police Department IT personnel)

1) Ensures all service packs and patches are current on mission-critical computers.
2) Ensures backups are in place for all critical systems.
3) Quarantine the system if necessary and practical.
4) Work with Information Security to determine the threat and risk.
5) Work with Information Security to determine the most effective remediation (cleanup or reimage).
6) Work with Information Security to determine if a forensic copy of the system's image is needed.
7) Continue to advise the Incident Handling Team of significant or suspicious events that may be related.
8) Forward all related notes or logs to the Incident Handling Team for integration into the Lessons Learned.

## V. Response to Computer Security Incident:

A. Preparation Phase

Incident response begins with the steps taken to protect our information resources before an incident takes place. This is done through end user awareness training, hardening of operating systems, installation of security tools, and the documentation of specific policies and procedures. Just as security affects everyone in the department at all levels, so should security safeguards be implemented at all levels.

B. Identification Phase

If we cannot detect incidents effectively, we cannot succeed in responding to incidents. Therefore, the detection of incidents phase is one of the most important aspects of incident response. It is also one of the most decentralized phases, in which those with incident response expertise have the least control. Initially, the incident may be reported by an end user, detected by a system administrator, identified by alerts, or discovered by many other means. An end user may report an incident through one of three avenues: their immediate supervisor, the Support Services Lieutenant or the police department IT personnel.

C. Containment Phase

Following the Identification Phase, the proper personnel and authorities need to be notified and further damage to the system must be prevented. Proper

personnel may include upper management, law enforcement, Local Agency Security Officer, or others as identified in the incident response procedures. Short-term containment actions to prevent further damage to the system might be disconnecting the network or power cable from system or applying filters to firewalls or routers. Immediately after the initial containment phase the Incident Response Team members gathers sufficient information about the incident to assess the impact and the appropriate long term response.

D. Eradication Phase

After an incident has been contained, eradication may be necessary to eliminate components of the incident, such as deleting malicious code and disabling breached user accounts. For some incidents, eradication is either not necessary or is performed during recovery.

E. Recovery Phase

System Administrators and other personnel restore systems to normal operation and (if applicable) harden systems to prevent similar incidents. Depending on the type on incident recovery may involve such actions as restoring systems from clean backups, rebuilding systems from scratch, replacing compromised files with clean versions, installing patches, changing passwords, and tightening network perimeter security.

F. Follow-up Phase

In this phase the Local Agency Security Officer and police department information systems employee sends incident reports to parties with a need-to-know, procedural changes and updates are discussed and if necessary an investigation is conducted to determine what the root cause and root effects of the incident.

## VI. Incident Classifications:

The importance of an incident might depend on many factors, and the priority can also change if new information is discovered or reported. So trying to establish and maintain a priority list of ongoing incidents is not easy and can in fact be a dynamic activity.

Regardless of priority, it may still be necessary to escalate an individual incident. The escalation of an incident is normally the result of an incident handler being unable to address one or more aspects of the incident appropriately. The incident handler ends up needing additional support or management oversight, or to offload other work in order to appropriately handle the escalated incident.

## VII. Contacts and Notification:

Each of the following areas will have a primary and alternate member:

a. Information Security Dept.
b. Internal Affairs
c. Legal
d. Local Agency Security Officer
e. Public/Media Relations

## VIII. Incident Review Report Template

A. Preparation

1. Were controls applicable to the specific incident working properly?
2. What conditions allowed the incident to occur?
3. Could more education of users or administrators have prevented the incident?
4. Were all of the people necessary to respond to the incident familiar with the incident response plan?
5. Were any actions that required management approval clear to participants throughout the incident?

B. Identification/Detection

1. How soon after the incident started did the organization detect it?
2. Could different or better logging have enabled the organization to detect the incident sooner?
3. Does the organization even know exactly when the incident started?
4. How smooth was the process of invoking the incident response plan?
5. Were appropriate individuals outside of the incident response team notified?
6. How well did the organization follow the plan?
7. Were the appropriate people available when the response team was called?
8. Should there have been communication to inside and outside parties at this time; and if so, was it done?
9. Did all communication flow from the appropriate source?

C. Containment

1. How well was the incident contained?
2. Did the available staff have sufficient skills to do an effective job of containment?
3. If there were decisions on whether to disrupt service to internal or external customers, were they made by the appropriate people?
4. Are there changes that could be made to the environment that would have made containment easier or faster?

5. Did technical staff document all of their activities?

D. Removal and Recovery

1. Was the recovery complete - was any data permanently lost?
2. If the recovery involved multiple servers, users, networks, etc., how were decisions made on the relative priorities, and did the decision process follow the incident response plan?
3. Were the technical processes used during these phases smooth?
4. Was staff available with the necessary background and skills?