Incident Response Plan
for PCI-DSS Compliance

City of Monroe, Georgia
Information Technology Division
Finance Department

I. Policy

The City of Monroe Information Technology Administrator is responsible for responding to reports of incidents, compromises, and breaches of City of Monroe computers, data, and network resources. The purpose of the Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements to address instances of unauthorized access to or disclosure of City information. The Incident Response Plan defines the policy, roles and responsibilities for the involved personnel when reacting to an information security threat.

The primary emphasis of activities described within this plan is the return to a secure state as quickly as possible, while minimizing the adverse impact to the City. Depending on the circumstances, the Information Technology Administrator (IT Administrator) may decide to modify or bypass one or more of the procedures outlined in this plan in response to a particular security incident, with the understanding that the IT Administrator will take all reasonable steps to investigate and resolve any security issues. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, as well as classification of the incident.

The City shall provide timely and appropriate notice to affected individuals and departments when there has been a security incident, a compromise, or a breach involving city data, computers, or networks. The IT Administrator, Finance Department Director, and the City Administrator shall be responsible for reviewing breaches to determine whether notification is required, and directing responsible departments in complying with the notification obligation. All known or suspected security incidents must be reported to the IT Administrator. Suspected incidents can be reported at administrator@monroega.gov or through the City of Monroe Call Center.

II. Definitions

Security Incident - A vulnerability which may compromise the security of city resources has been discovered and is underway. Generally, this means a weakness in intrusion prevention has been found, an attempted exploit has taken place, or reconnaissance by a hacker has been thwarted. Examples include systematic unsuccessful attempts to gain entry, a PC or workstation infected with a virus, worm, Trojan, botnet, or other malware that has been discovered and removed.

Security Compromise – An escalation of a security incident where the attacker has gained control of a city account, system, or device, and is leveraging that position to control and utilize compromised resources for the purpose of unauthorized acquisitions. At this point, it has been determined that data has not been compromised or stolen.

Security Breach – A confirmed, unauthorized acquisition, modification or destruction of city or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.

Private data - Data about individuals that is classified by law as private or confidential and is maintained by the city in electronic format or medium. “Private data” means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

Unauthorized acquisition - For the purposes of this plan, this means that a person has obtained city data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-city purposes

Systematic unsuccessful attempts - continual probes, scans, or login attempts where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

City of Monroe Resources **or** ***Systems*** includes all city-owned computers, peripherals, networks, and related equipment and software, and the voice and data communications infrastructure.

III. General Incident Response Procedures

1) Intrusion attempts, security breaches, or other technical security incidents perpetrated against city-owned computing or networked resources must be reported to the IT Administrator. Functional unit managers and/or supervisory personnel must:

a) Report any security incidents in order to obtain assistance, advice, or to file the incident.
b) Report any systematic unsuccessful attempts (e.g., login attempts, probes, or scans).
c) Where feasible given the circumstances, reports should be sent as soon as the situation is detected; minimally the report should be sent as soon as possible thereafter.

2) Upon receiving a report of a security incident, the IT Administrator will:

a) Ensure that appropriate information is collected and logged per applicable procedures.
b) Immediately assess actual or potential disclosure or inappropriate access to institutional or personal information.
c) Report the situation to the Finance Director and/or City Administrator.
d) Consult with and/or assign the incident to other personnel for further investigation as necessary.
e) Provide preliminary advice or comment to the functional unit as required.
f) Initiate steps to warn other City of Monroe systems personnel if it appears that the situation has the potential to affect other city systems as well.
g) Perform or assist in any subsequent investigation and/or perform computer forensics as required.
h) If circumstances dictate, report and/or consult with city Legal Counsel, city Police, Internal Auditors, city Public Relations, or other appropriate agencies.
i) Ensure that appropriate records are filed.
j) Confirm actual or probable disclosure or inappropriate access to institutional or personal information.
k) Invoke formal incident response procedures commensurate with the situation.

3) In order to protect city data and systems, as well as to protect threatened systems external to the city, the IT Administrator may block, or place restrictions on technology services provided using any city owned systems and networks. Specifically:

a) Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.
b) Restrictions may be permanently deployed based on a continuing threat or risk after appropriate consultation with affected constituents, or they may be temporarily deployed, without prior coordination, in response to an immediate and serious threat.
c) Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the affect on city functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the IT Administrator.

4) In order to protect city data and systems, as well as to protect threatened systems external to the city, the IT Administrator may unilaterally choose to isolate a specific city system from other city or external networks, given:

a) Information in-hand reasonably points to the system as having been compromised.
b) There is ongoing activity associated with the system that is causing or will cause damage to other city systems and/or data, or the assets of other internal or external agencies, or where there is a medium-to-high risk of such damage occurring.
c) All reasonable attempts have been made to contact the responsible systems personnel or department management, or such contact has been made where the technician or department managers are unable to (or choose not to) resolve the problem in a reasonable time.
d) Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the IT Administrator.
e) Advance consultation with the appropriate security contractor, or Legal Counsel, where practical and where circumstances warrant.

5) The reaction to a reported security vulnerability directly corresponds to the potential for damage to the local system (or adjacent systems) or inappropriate disclosure or modification of data. The risk levels are characterized as:

a) Very High Risk, response is immediate:

    1. Damage to the system or data is occurring, or
    2. Attempts to exploit the vulnerability on that system are occurring, or
    3. The vulnerability is currently being actively exploited against other similar technologies within the City; probable damage to systems and data is being experienced in those other incidents.

b) High Risk, response is within 1 hour:

1. The vulnerability is known to exist on the system;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. Damage to systems and data are being experienced in those other incidents.

c) Medium Risk, response should be within 4 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. There is some potential for damage to systems and data.

d) Low Risk, response should be within 8 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. Damage to systems and data is possible but is not considered likely.

6) In the event of a significant series of incidents, a compromise, or a breach, the entire episode and response are reviewed to determine which parts of the incident response plan worked correctly. The "lessons learned" will be part of an After Action Review to determine areas that need to be changed (policies, system configurations, etc.).

IV. Procedures for System Users and Administrators

1) **Don't panic.** Be as calm and methodical as you can, and think about your course of action. Involve a second person to assist and observe all actions you take.

2) **Do a quick assessment.** Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. If this does not appear to be the case, leave the system intact for the moment.

3) **Report the problem.** Call the IT Administrator or the City of Monroe Call Center, and request an emergency system security check. Every effort will be made to respond as quickly as possible, as well as, respect the confidentiality of incident information.

4) **Gather all the relevant information you can find.** This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and activity logs. Copy them to a safe location (that will not be deleted or over-written), so that we can study them later.

5) **Take notes.** Have your partner record all relevant information, including things you observed, actions you took, dates and times, and the like. It is best to log your activities as they occur. Over time, your actions and the order in which they were executed will not be easily remembered. The preservation of information is critical to any legal action that may take place at a later date.

6) **Change account passwords.** All system accounts that were involved with the incident should have new passwords requested. Exceptions to this rule are accounts which are authenticated with tokens or certificates, in which case the PIN or pass-phrase for them should be changed. **Never** share your password (pin, or pass-phrase) with anyone, for any reason.

7) **Change the status of accounts, if necessary.** In the event that a system administrator detects a problem with a system, or user activity on a system, a quick way to stop the unwanted activity is to "disable" an account, by restricting logins to it. This is *not* deleting the account, but is merely making the account temporarily unusable through Active Directory.

8) **Stop rogue service(s), if necessary.** In the event that a system compromise or denial-of-service attack is underway, and you are unable to stop or kill the service(s), you may need to disconnect the machine from the network to get them stopped.