Incident Management Policy

1. **PURPOSE**
   This policy defines agency responsibilities for responding to and reporting cyber intrusion and for sharing information related to potential incidents or threats with the South Carolina Information Sharing and Analysis Center (SC ISAC).

2. **SCOPE**
   This Policy applies to agencies, departments, commissions, and boards (herein referred to as “agencies”) that receive, expend or disburse State funds or incur obligations for the State. This policy does not apply to colleges and universities. However, they are encouraged to comply due to the frequent need to access and exchange data with the agencies.

3. **POLICY**
   To secure and protect the South Carolina’s critical information technology (IT) business processes and assets from cyber-crime or cyber-terrorism, State agencies should report all cyber intrusion to the SC ISAC. The agency’s Assigned Designated Approving Authority (DAA), should appoint a coordinator to work with the SC ISAC.

4. **Cyber Intrusion:** Agencies should report any of the following acts by any person who, without authority or acting in excess of authority:
   - Accesses an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network.
   - Accesses, alters, damages, or destroys any IT device, network, or any physically or logically connected IT devices.
   - Accesses, alters, damages, or destroys any computer application systems, programs, or data.
   - Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network.
   - Denies or causes the denial of IT-related services to any authorized user of those services.
   - Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person.
   - Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system.
   - Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, or on behalf of the State, a political subdivision of the State, or a medical institution.
Incident Management Policy

- Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network.
- Makes multiple attempts to access an IT device or network system within a brief period of time.

4.1. **Cyber Intrusion Reporting** – The agency should notify SC ISAC within one hour of detecting the intrusion by whatever means of communication is both available and fastest (i.e., phone, fax, e-mail, courier).

- The following information, at a minimum, is required when reporting intrusions to SC ISAC:
  a. Agency name
  b. The Agency SC ISAC Coordinator's name and phone number
  c. Brief description of intrusion and damages (real or anticipated)

- Whenever possible, the agency should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

4.2. **SC ISAC Incident Report** – After notifying SC ISAC of the intrusion, the agency’s coordinator should complete a SC ISAC Incident Report (see Attachment A) available from [http://secure.sc.gov/site/Incident%20Reporting.asp](http://secure.sc.gov/site/Incident%20Reporting.asp). The agency’s coordinator completing the report should provide as much detail as possible in the remarks fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the agency’s coordinator should revise and re-submit the incident report to SC ISAC with a clear date-time stamp.

4.3. **SC ISAC Activity** – Depending on the reported damage from the intrusion, SC ISAC will be in constant contact with the agency’s coordinator at the affected agency, CIO, South Carolina Law Enforcement Division (SLED), Attorney General’s Office, and other organizations, as necessary, until resolution and recovery efforts are completed.

4.4. **Alert Notifications**

4.4.4. **SC ISAC Responsibilities** – As SC ISAC creates or receives computer security alerts, it should determine whether to send it to "All Agencies" or specific Agencies, or only to specific individuals, depending on the security alert. Each alert should state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.
Incident Management Policy

4.4.5. **Agency Responsibilities** -- Upon receiving a SC ISAC Alert, agency SC ISAC Coordinators should notify agency personnel about the alert.

4.5. **SC ISAC Membership Form** -- Agency SC ISAC Coordinators should complete a SC ISAC Membership Form (see Attachment B) and deliver it to SC ISAC. Agency SC ISAC Coordinators should ensure that the contact information on the form remains current and apprise SC ISAC of any changes.