

## ***Rules of Engagement***

Agencies must report information security incidents to the SIRT within the timeframe specified by the statewide Incident Response policy. Upon contact, the SIRT will assign an incident coordinator and assess the severity and impact of the incident. If needed or requested, the SIRT may perform various roles in responding to the incident, including incident command, physical response, forensic analysis, or other roles as needed.

When responding to an incident with an agency, the following are rules of engagement between SIRT and agencies:

- Mutual respect of authority and business requirements.
- Agencies will advise the SIRT of potential incidents in a timely manner.
- SIRT may request or require problem hosts or networks be disconnected from the statewide network and/or the Internet if needed for containment.
- Agency computer resources may be quarantined for forensic investigation.
- Agency management will be briefed as much in advance as possible prior to implementing actions affecting agency business.
- Agencies will provide resources to assist the SIRT to expedite investigations, containment, and resolution of an incident.
- SIRT will work with agencies to determine if and when external resources will be notified.
- Agency and SIRT staff will work collaboratively.
- Agencies and SIRT will maintain clear communications between incident responders.
- Agencies and SIRT will work in accordance with state and agency policies.
- SIRT may require agencies to implement mitigating actions (e.g. patches, firewall rules) in a timely manner.
- Agencies and SIRT will work together on post incident activities such as remediation and lessons learned.

Because of the sensitivity of incident information, the SIRT will adhere to the following practices regarding agency information:

- Default classification level for all communications within SIRT will be level 2 (as defined in the statewide Information Asset Classification policy 107-004-050). SIRT members will reinforce this message as appropriate with other participants during an incident.
- Information not to be shared outside incident meetings must be identified by agency personnel and will not be included in minutes or any other media that might become public record or be otherwise released.
- Potentially public information brought to the SIRT will not be shared without specific discussion and authorization.
- Information about an incident will not be released to any unauthorized party.
- When it is deemed by the SIRT that technical details of an incident will benefit other state agencies or the public as a whole, redacted details of the incident will be shared as it is deemed appropriate and confidentiality can be preserved.