15.0 INCIDENT RESPONSE

15.1 Purpose

The purpose of this policy is to set the standards and procedures for security incident determination and response.

15.2 Policy

15.2.1 Incident and Breach Definitions

A “Breach” is defined in Ga. Code § 10-1-910 et seq. as an unauthorized acquisition of an individual’s electronic data that compromises the security, confidentiality, or integrity of Personal Information (PI) of such individual maintained by an Entity. Good-faith acquisition or use of PI by an employee or agent of an Entity for the purposes of such Entity is not a breach of the security of the system, provided that the PI is not used or subject to further unauthorized disclosure.

An “Incident” is any security event (or collection of them) that activates the alert process in this policy; they are any information system related event involving a violation of the law, or a violation of security policy. Such an incident may alternatively involve any significant disruption of operational operations or any event that seriously jeopardizes the security or privacy of classified FCS data or assets. Incidents will be determined by the Alert Process Tree listed below. Incidents must be logged and documented in a Computer Security Incident Response (CSIR) Report.

A “Security Event” is any occurrence of a user, application, system, or network function that could be relevant to the security posture of FCS. The vast majority of these will not be relevant to cybersecurity but must be logged and correlated by security tools for correlation to potential incidents.

15.2.2 Reporting

All users of FCS information systems and assets must be trained and prepared to report any violation of this policy or suspected security incidents to the Technology Department by:

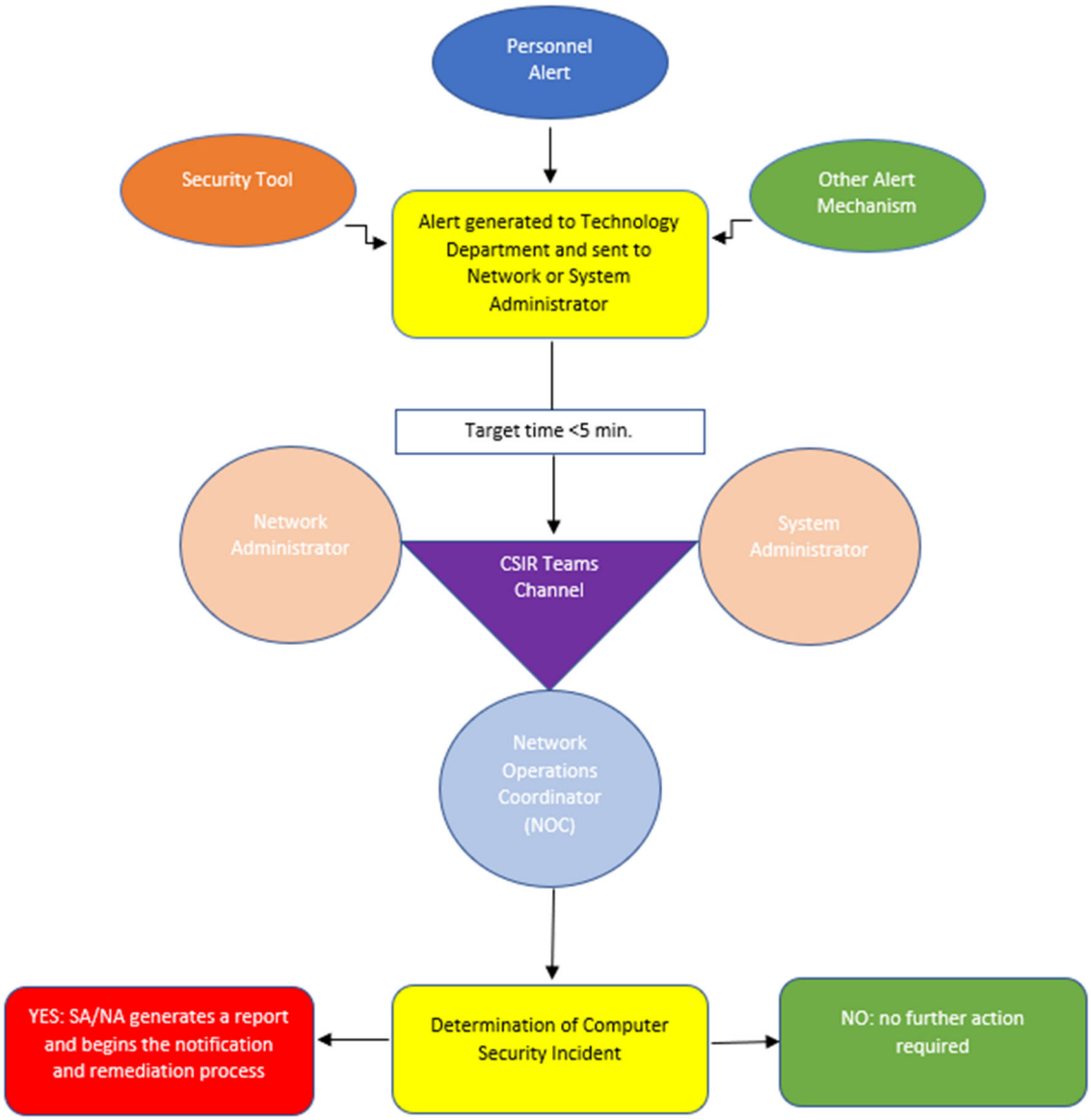
Alerting their immediate supervisor or ITS

All users are responsible for the cybersecurity of FCS and must be trained and prepared to report security events.

15.2.3 Alert Process

The following is how Security Events will be categorized into one of the definitions above. Security Events will be delivered to the Technology Department through security tool alerts, personnel reporting, technical discovery, or many other forms. The Network and Systems Engineers (NE and SE) as well as the Network Operations Coordinator (NOC) will serve on the Computer Security Incident Response (CSIR) Team. The NOC will maintain a Microsoft Teams channel that will serve as the primary means of communication and coordination for security incidents and determination. When an event enters the TD, one of the parties above will investigate the event to determine if the CSIR need to determine if an impact to FCS data or critical assets has possibly occurred. The CSIR will meet on a Microsoft Teams meeting at the soonest possible time to determine if FCS classified data or a critical asset may have been affected. In the event a definitive Breach, Incident or Security Event is identified, the NOC or Director of Technology Services will notify the CTIO, who will then notify the Superintendent and Public Relations Director. The process to define the event as an Incident or Breach is shown below:

Computer Security Incident Report Generation:



Alerts from security tools for Events that meet a threshold of Critical will be reviewed by the Network Operations Team and will generate an alert to the CSIR via email. The Event will be reviewed by the responsible administrator and either elevated to the CSIR Teams channel or dismissed as a false positive. If the administrator believes the Event may be accurate, the administrator will raise the issue in the Teams CSIR channel, and the NOC will determine if an Incident or Breach has occurred.

15.2.4 Incident Documentation

All Security Events that are determined to be an Incident or Breach will be documented in a Computer Security Incident Response form. The form will be saved in the CSIR Teams Channel in documentation. The applicable administrator will be responsible for creating and maintaining the document for the duration of the incident. The CSIR form will be based on the requirements of NIST SP 800-61r2 and will have the following sections:

- Executive Summary
- Impact Assessment
- Timeline
- Technical Data
- Comments
- Figures (as applicable)

Once a CSIR has been started, the document will be classified as **RESTRICTED** and will only be used by personnel involved that have a need to access the document.

15.2.5 Incident Closure

All Security Incidents and Breaches will remain open or in progress until the CSIR Team has sufficient evidence to determine that the adverse condition to FCS classified data or critical assets has been halted. Once the Incident or Breach has been closed, the responsible administrator will fill out the remaining sections of the document and the DOT will schedule a briefing for the CTIO to review:

- Incident or Breach Summary
- Impact to Assets and Data
- Actions Taken to Close the Incident or Breach
- Lessons Learned
- Next Steps

The CTIO will be responsible for briefing the Superintendent and/or BOE if the incident does cause serious affect to FCS classified data or critical assets.

15.2.5 Incident Response Procedures

15.2.5.1 Classified Data Exposure

All Data Custodians of classified FCS data will implement (where possible) Data Loss Prevention (DLP) mechanisms to alert the custodian of any form of misuse of the data. Misuse of the data could include but is not limited to:

- Unauthorized Access
- Unauthorized Destruction
- Unauthorized Alteration
- Unauthorized Exfiltration
- Unauthorized Storage
- Personnel Errors

Any alert to the possible misuse of FCS data classified at or above **CONFIDENTIAL** must be reported to the CSIR Team immediately for a determination of a Breach or Incident.

Upon discovery of an alert to the misuse of FCS classified data the Data Custodian must investigate the Event to determine if the alert is valid or not. If the alert is valid, the Data Custodian must take immediate action to stop the misuse of the data or ask for help from the CSIR or Physical Security personnel. Once the Data Custodian has sufficient evidence to verify that the misuse of the data has ceased, the Data Custodian will assist the CSIR in documenting the incident in a CSIR Report. Data Custodians immediate supervisors are responsible for briefing the Superintendent and notification requirements.

15.2.5.2 Information System and Network Incidents or Breaches

The Network Operations team is responsible for determining if Security Events are worth elevating to the CSIR Team for determination of an Incident or Breach. The applicable administrator will be responsible for

taking action to halt any Breach or Incident to a critical information system asset. Once a Security Event has been investigated, the SA or NA will take action to reduce the effect of the event. If the asset is critical, the Director of Technology Services or NOC will make the decision to act on the critical asset. To gather information on the incident, the responsible administrator should:

- Gather initial evidence, including logs and alerts.
- Determine the current and potential technical effect of the incident.
- Determine the criticality of the affected resources.
- Determine the general state of the network overall.
- Determine if malicious or non-malicious in origin (worm vs. configuration error or hardware failure.)
- Determine if internal or external in origin.
- Determine if attempting to propagate.

If possible, affected systems and network objects should be preserved for evidence and investigation, but this should not take priority over stopping the Breach or Incident.

15.2.5.3 Recovery

Each asset classified as CRITICAL in the Business Continuity Plan (BCP) will have a procedure for recovery in the Disaster Recovery Plan. Disaster Recovery Plans must be tested for operational capability. All disaster recovery procedures must have a primary and secondary employee that are prepared to implement the disaster recovery procedure.

15.2.6 Notification

If a Security Event has been determined to be a Breach (In Accordance With [IAW] Ga. Code § 10-1-910 et seq.) the CSIR Team will include legal counsel to determine legal breach notification requirements. All external Breach notifications or Incident communications will be conducted through the Communication and Community Engagement Office. All internal Incident and Breach communication and notification will be conducted through the Technology Department. Data surrounding security Events, Incidents, and Breaches should only be shared with the necessary parties and should be limited to the data that is relevant to their position. All data should be shared with necessary parties to include the lessons learned and next steps for prevention in the future. Public announcements and relations will be managed by the Communications Office.

16.0 INTERNAL EVALUATION

16.1 Purpose

The purpose of this policy is to set the standards for internal evaluation of FCS procedures and controls.

16.2 Policy

16.2.1 Security Assessments

At least every other year, the FCS Technology Services Department will conduct a security assessment or penetration test to verify the efficacy security controls in place. The test should include an assessment of the FCS network and information systems. All assets and applications classified in the BCP as CRITICAL will be included in some form of security assessment. In cases where a third party manages an asset, the third-party will be required, unless given a variance by FCS, to demonstrate proof that a security assessment or penetration test was conducted. Applications that process data classified at or above **CONFIDENTIAL** must undergo application security assessments as well as infrastructure. All security controls should be tested at least annually to ensure they are operating properly. An adversarial exercise should be conducted at least every other year to test detection, incident response, and recovery capabilities.

16.2.2 Evidence

All Asset Managers responsible for FCS assets or data must maintain evidence that they meet the requirements of the NIST CSF. For assets and applications that are managed by a third-party, the applicable asset manager must maintain evidence that the third-party conducts and remediates annual security assessments. Annually, each of the requirements of the NIST CSF will be assessed for continued compliance.

16.2.3 Improvement

All assessments, tests, Incidents, and Breaches will be used to improve the detection, alerting, and response functions of FCS. The NOC will be responsible for coming up with the plan to alter the processes of FCS.

16.2.4 Policy and Procedures Review

Annually, the Director of Technology Services or NOC will review all policies, procedures, and plans for accuracy and needed updates. The personnel responsible for the review and update must log the changes in the Version and Revision section of the document including a summary of the changes made.