Scope

The Statewide Information Security Policies are the foundation for information technology security in North Carolina. The policies set out the statewide information security standards required by N.C.G.S. §143B-1376, which directs the State Chief Information Officer (State CIO) to establish a statewide set of standards for information technology security to maximize the functionality, security, and interoperability of the State's distributed information technology assets, including, but not limited to, data classification and management, communications, and encryption technologies. These standards apply to all executive branch agencies, their agents or designees subject to Article 15 of N.C.G.S. §143B. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

This policy document provides the State of North Carolina's (State) security policy statements for the Incident Response program that shall be implemented and maintained by identified covered personnel for the prevention of, reporting of, investigation of, and remediation of information security incidents impacting information systems and data of which the State is considered the owner.

Responsibilities

All covered personnel that utilize IT resources are responsible for adhering to this policy and with any local Incident Response requirements based on their assigned responsibilities defined below.

Role	Definition
Agency Management	The State Chief Information Officer (SCIO), Agency Chief Information Officer (CIO), Chief Information Security Officer (CISO), or other designated agency officials at the senior leadership level are assigned the responsibility for the continued development, implementation, operation and monitoring of the Incident Response program.
Incident Response Officer	The Incident Response Officer (IRO) is a senior or executive level individual such as the CISO, CIO or Agency Security Liaison who is accountable for the actions of the IR team and the IR function.
Incident Response Manager	Reporting to the IRO, the Incident Response Manager (IRM) is responsible for leading the efforts of the Incident Response Team (IRT) and coordinates activities between all of its respective groups. The IRM is responsible for activating the IRT team and managing all parts of the IR process, from discovery, assessment, remediation and finally resolution. This role typically resides with the Enterprise Security and Risk Management Office (ESRMO).
Incident Response Team (IRT)	Reporting to the IRM, the IRT is comprised of representatives from IT, Security, Application Support and other business areas. Members of a IRT are responsible for providing accelerated problem notification, containment, and recovery services in the event of computer security related emergencies, such as virus infections, unauthorized

	access, or other events that may compromise production systems or information. All information security incidents must be handled with the involvement and cooperation of NCDIT.
Local Incident Response Coordinator	Reporting to the IRM, the Local Incident Response Coordinator (LIRC) is the Agency Security Liaison. This person is recognized as the local IR leader and is able to direct efforts of the local incident responders during an incident and provide status updates to the IRM
Incident Responders	Reporting to the IRM or the LIRC during an incident depending on their location, these technical experts are identified and called upon to assist in the remediation and resolution of a given incident.
Covered Personnel	Covered personal have the responsibility to report information technology security incidents, software errors or weaknesses to agency management in accordance with statewide information security standards and agency standards, policies, and procedures. The notification shall be made as soon as possible after the weakness is discovered.
Third Parties	Third party service providers must provide Incident Response plans and capabilities that meet State requirements. Third parties are required to maintain and update their plans on an annual basis or when there is a change in business requirements. Incident Response plans are subject to periodic review of incident response controls by the State.

IR-1 - Policy

The requirements described in this Incident Response policy are designed to help agencies respond to, and minimize the impact of cybersecurity incidents of information systems and data of which the State is considered the owner.

The State has adopted the Incident Response principles established in NIST SP 800-53 Rev 4 “Incident Response” control guidelines as the official policy for this security domain. The "IR" designator identified in each procedure represents the NIST-specified identifier for the Incident Response control family. The following subsections in this document outline the Incident Response requirements that the State and agencies must develop, or adhere to in order to be compliant with this policy. This policy shall be reviewed annually, at a minimum.

IR-2 - Incident Response Plan Training

Agencies must train personnel with access to the State network in their incident response roles. The agency must provide incident response training to information system users consistent with assigned roles and responsibilities. Agencies shall do the following:

a. Provide training prior to assuming an incident response role or responsibility, when required by information system changes, and annually thereafter.

b. Provide additional or supplemental IR training when information system changes occur.

c. Include user incident response training regarding the identification and reporting of suspicious activities, both from external and internal sources.

d. Maintain a comprehensive record of all IR related training. The electronic log shall include names of participants, information system name(s), type of training, and date of completion. Log entries shall be maintained by the Agency Security Liaison or designee.

IR-3 - Incident Response Plan Testing

All agency incident response personnel and service providers must perform the following testing:

a. Identify essential missions and business functions and associated incident response requirements.

b. Agencies must perform tabletop exercises using scenarios that include a breach of restricted or highly restricted data and should test the agency's incident response policies and procedures.

c. A subset of all employees and contractors with access to restricted or highly restricted data must be included in table top exercises.

d. Each tabletop exercise must produce an after-action report to improve existing processes, procedures, and policies.

e. Agencies entrusted with restricted or highly restricted data must test the incident response capability at least annually.

f. For systems that store, process or transmit federal tax information (FTI), see Section 10.3, Incident Response Procedures in IRS 1075, for specific instructions on incident response requirements.

g. This control is optional for LOW risk information systems.

IR-3 (2) - Incident Response Plan Testing – Coordination With Related Plans (Moderate Control)

The agency shall coordinate incident response testing with agency elements responsible for related plans. Agency plans related to incident response testing include, for example, Business Continuity Plans, Disaster Recovery Plans, Continuity of Operations Plans (COOP), Crisis Communications Plans, Critical Infrastructure Plans, and Occupant Emergency Plans.

IR-4 – Incident Handling

The State shall protect technology resources by conducting proper investigations:

a. The IRM, acting on behalf of the SCIO, shall evaluate the proper response to all information technology security incidents reported to the agency.

b. The IRM shall work with agencies to decide what resources, including law enforcement, are required to best respond to and mitigate the incident.

c. After the initial reporting and/or notification, agency management shall review and reassess the level of impact that the incident created.

d. The IRM shall coordinate incident handling activities with contingency planning activities.

e. An investigation into an information technology security incident must identify its cause, if possible, and appraise its impact on systems and data. The extent of damage must be determined and course of action planned and communicated to the appropriate parties.

f. Agencies shall investigate information system failures to determine whether the failure was caused by malicious activity or by some other means (i.e., hardware or software failure).

g. If any suspicious activities are detected, responsible personnel within the affected agency shall be notified to ensure that proper action is taken.

h. Agencies shall establish controls to protect data integrity and confidentiality during investigations of information technology security incidents. Controls shall either include dual-control procedures or segregation of duties to ensure fraudulent activities requiring collusion do not occur.

i. Evidence of or relating to an information technology security breach shall be collected and preserved in a manner that is in accordance with State and federal requirements.

j. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities to ensure the evidence is properly preserved for any legal actions that may ensue as a result of the incident.

k. Any system, network, or security administrator who observes an intruder on the State network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.)

l. In the event of an active incident, agency management has the authority to decide whether to continue collecting evidence or to restrict physical and logical access to the system involved in the incident. Note: It may be necessary to isolated from the network until the extent of the damage can be assessed.

m. When dealing with a suspected incident, agencies shall do the following:

i. Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.

ii. Make copies of all audit trail information such as system logs, network connections (including IP addresses, TCP/UDP ports, length, and number), super user history files, etc.

iii. Take steps to preserve and secure the trail of evidence.

n. The agency's CIO or his/her designee will determine if other agencies, departments, or personnel need to become involved in resolution of the incident. Agencies shall consider coordinating IR activities with external organizations, such as the OSA, OSHR, SBI, or the FBI.

o. Agencies shall require all personnel directly involved with incident handling to have signed a Non-Disclosure Agreement (NDA).

p. Agencies shall discuss incident details only on a need-to-know basis with authorized personnel.

q. When responding to a malware threat, agencies shall perform the following tasks:

i. Verify threats to rule out the possibility of a hoax before notifying others

ii. Identify personnel responsible for mitigation of malware threats

iii. Have internal escalation procedures and severity levels

iv. Have processes to identify, contain, eradicate, and recover from malware events

v. Have a contact list of antivirus software vendors

r. Agencies may utilize the following for guidance regarding incident handling:

i. NIST SP 800-36, Guide to Selecting Information Technology Security Products;

ii. NIST SP 800-61, Computer Security Incident Handling Guide, Revision 2;

iii. NIST SP 800-83, Guide to Malware Prevention and Incident Handling for Desktops and Laptops, Revision 1;

iv. NIST SP 800-86, Guide for Integrating Forensic Techniques into Incident Response;

v. NIST SP 800-92, Guide to Information Security Log Management;

vi. NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS);

vii. NIST SP 800-101, Guidelines on Mobile Device Forensics, Revision 1; and

viii. Other appropriate guidance, as necessary.

s. Agencies shall activate and implement a security incident handling capability during all stages of the NIST incident response life cycle (See Figure 1), including the following:

i. Preparation

ii. Detection and Analysis

iii. Containment, Eradication, and Recovery

iv. Post-Incident Activities

Figure 1

t. All agencies shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals as determined by agency management.

u. All agencies shall maintain records of information security breaches and the remedies used for resolution as references for evaluating any future security breaches. The information shall be logged and maintained in such a location that it cannot be altered by others. The recorded events shall be studied and reviewed regularly as a reminder of the lessons learned.

v. The agency/department IT manager and/or incident response coordinator shall determine the criticality of an incident (see IR-6 for severity levels).

w. Agencies shall enact automated processes for the purpose of correlating security events, e.g. Security Information and Event Management (SIEM) technology.

x. Lessons learned from incident handling activities shall be incorporated into incident response procedures, training, and testing/exercises, and implements the resulting changes.

y. Agencies shall create processes to provide information for the enhancement of organizational and Agency information security awareness programs and incident response programs.

IR-5 - Incident Monitoring

Maintaining records about each information system incident, the status of the incident, and other pertinent information is necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.

a. Agencies shall track and document information system security incidents potentially affecting the confidentiality of all other restricted and highly restricted data.

b. If the incident is rated a severity 3 or higher (see IR-6 for severity levels), subsequent reports to agency management shall be provided.

c. Agencies shall monitor and control the release of confidential security information during the course of a security incident or investigation to ensure that only appropriate individuals have access to the information, such as law enforcement officials, legal counsel or human resources

d. A follow-up report shall be submitted to agency management upon resolution by those directly involved in addressing the incident and contain the following:

   i. Point of contact

   ii. Affected systems and locations

   iii. System description, including hardware, operating system, and application software

   iv. Type of information processed

   v. Incident description

   vi. Incident resolution status

   vii. Damage assessment, including any data loss or corruption

   viii. Organizations contacted

   ix. Corrective actions taken

   x. Lessons Learned

IR-6 - Incident Reporting

To increase effectiveness in assessing threat levels and detecting patterns or trends in regard to information technology security incidents through proper documentation all computer security incidents. Security incidents, for example, suspicious events (e.g. insider threat), software errors or weaknesses, system vulnerabilities associated with security incidents (e.g. Ransomware), and lost or stolen State computer equipment, shall be reported *immediately* to the agency management.

a. Agencies shall ensure all suspected security incidents or security breaches are reported to the ESRMO within twenty-four (24) hours of incident confirmation, as required by NC general statute. Agencies shall report incidents to the ESRMO by one of the following methods:

   i. Contact DIT Customer Support Center 800-722-3946

   ii. Use the incident reporting website https://it.nc.gov/cybersecurity-situation-report.

   iii. Contact a member of the ESRMO staff directly by phone or email security@its.nc.gov.

b. For incidents involving FTI, agencies shall contact the appropriate special agent-in-charge, TIGTA, and the IRS Office of Safeguards *immediately* but no later than 24 hours after identification of a possible issue involving FTI. Refer to IRS 1075 Section 10.0, Reporting Improper Inspections or Disclosures, for more information on incident reporting requirements.

c. For reporting security incidents to outside authorities, agencies shall do the following:

   i. Agencies shall coordinate with ESRMO in accordance with the State's Incident Response Plan, applicable state laws, procedures, and agreements that require reporting to the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor. Agencies shall report all security incidents to the ESRMO when reported to an outside entity.

   ii. Agencies shall notify the Social Security Administration (SSA) Regional Office and their SSA Systems Security Contact within one (1) hour of suspecting loss if a privacy or security incident involves the unauthorized disclosure of Social Security data. If the security incident is related to the State Transmission/Transfer Component (STC) and the agency is unable to notify the SSA Regional Office or the SSA Systems Security Contact within 1 hour, the STC must report the incident by contacting SSA's National Network Service Center (NNSC) at 1-877-697-4889. Refer to the statewide Privacy Policy, NC-SEC-318-00, for additional guidance.

   iii. If a security incident involves the possible breach of FTI, the agency must contact the appropriate special agent-in-charge, the Treasury Inspector General for Tax Administration (TIGTA), and the IRS Office of Safeguards immediately, but no later than twenty-four (24) hours after identification.

   iv. Agencies shall notify consumers in the event of a security breach resulting in the unauthorized release of unencrypted or un-redacted records or data containing personal information with corresponding names. **Note**: The acquisition of encrypted data is only a breach if a confidential process or key needed to unlock the data is also breached, or if the data is encrypted by an unauthorized or malicious process, such as ransomware.

   v. The agency CIO and/or his/her designee shall manage the dissemination of incident information to other participants, for example law enforcement or the press. Public release of information concerning a security incident shall be coordinated through the agency's CIO, the Incident Response Team (IRT), and the agency's Public Information Officer (PIO).

d. Information recorded in regard to information technology security breaches shall cover the following at a minimum:

   i. Identify the current level of impact on agency functions or services (Functional Impact).

   ii. Identify the type of information lost, compromised, or corrupted (Information Impact).

iii. Estimate the scope of time and resources needed to recover from the incident (Recoverability).

iv. Identify when the activity was first detected and when corrective actions were implemented.

v. Identify the number of systems, records, and users impacted.

vi. Identify the network location of the observed activity.

vii. Identify point of contact information for additional follow-up.

viii. Identify the attack vector(s) that led to the incident.

ix. The method of breach detection and incident response actions

x. Provide any indicators of compromise, including signatures or detection measures developed in relationship to the incident.

xi. Provide any mitigation activities undertaken in response to the incident.

Incident Severity Levels

The Incident Response Manager (IRM) is responsible for initially assessing an incident's impact, and assigning a severity to the incident. This initial severity assignment dictates the level of response to the incident. As response to the incident progresses, it may be determined that the incident is more (or less) severe than originally realized, and a new severity level assigned. Security incidents are divided into five levels of severity based on their potential to negatively impact North Carolina agency operations, finances, and/or reputation. The characteristics in the table below should be used as baseline severity levels and may include additional threats categories.

Incident Severity	Incident Characteristics
5 **GENERAL ATTACK(S)** **SEVERE**	• Potential for or actual loss of lives or significant impact on the health or economic security of the state • Significant risk of negative financial or public relations impact • Loss of critical supervisory control and data acquisition (SCADA) systems • Successful penetration or denial-of-service attack(s) detected with significant impact on North Carolina state network operations: ○ Very successful, difficult to control or counteract ○ Large number of systems compromised ○ Significant loss of confidential data ○ Complete network failures ○ Mission-critical system or application failures ○ Compromise or loss of administrative controls of critical system

4 **LIMITED ATTACK(S)** **HIGH**	• Low risk of negative financial or public relations impact • Widespread instances of a computer virus or worm that cannot be handled by deployed anti-virus software • A critical vulnerability is discovered but no exploits are reported A critical vulnerability is being exploited but there has been no significant impact • Penetration or denial-of-service attack(s) detected with limited impact on State network operations: ○ There are credible warnings of increased probes or scans ○ Minimally successful, easy to control or counteract ○ Small number of systems compromised ○ Little or no loss of confidential data ○ No loss of mission-critical systems or applications ○ A compromise of non-critical system(s) did not result in loss of data
3 **SPECIFIC RISK OF ATTACK** **ELEVATED**	• An exploit for a critical vulnerability exists that has the potential for significant damage • A critical vulnerability is being exploited and there has been a moderate impact • There is a compromise of a secure or critical system(s) containing sensitive information • There is a compromise of a critical system(s) containing non-sensitive information, if appropriate • Widespread instances of a known computer virus or worm, easily handled by deployed anti-virus software • Isolated instances of a new computer virus or worm that cannot be handled by deployed anti-virus software • There is a distributed denial of service attack. • Significant level of network probes, scans and similar activities detected indicating a pattern of concentrated reconnaissance
2 **INCREASED RISK OF ATTACK** **GUARDED**	• A critical vulnerability is discovered but no exploits are reported. • A critical vulnerability is being exploited but there has been no significant impact. • A new virus is discovered with the potential to spread quickly. • There are credible warnings of increased probes or scans. • A compromise of non-critical system(s) did not result in loss of data. • Small numbers of system probes, scans, and similar activities detected on internal systems • External penetration or denial of service attack(s) attempted with no impact to State network operations • Intelligence received concerning threats to which State NCDIT systems may be vulnerable
1 **LOW**	• Small numbers of system probes, scans, and similar activities detected on internal and external systems • Isolated instances of known computer viruses or worms, easily handled by deployed anti-virus software • Unsubstantiated or inconsequential event

IR-7 - Incident Response Assistance

The ESRMO shall provide incident response support that offers advice and assistance to users of State and agency managed information systems for the handling and reporting of security incidents. These resources may include digital forensic services, vulnerability assessments, and incident response capability. Agencies shall establish and maintain a cooperative relationship between its IR capability and the State's IR capability, and other external, key providers of information systems.

IR-8 - Incident Response Plan

Agency missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. All agency Incident Response plans must include the following requirements:

a. Provides the agency with a roadmap for implementing its incident response capability,

b. Describes the structure and organization of the incident response capability,

c. Provides a high-level approach for how the incident response capability fits into the overall agency,

d. Meets the unique requirements of the agency, which relate to mission, size, structure, and functions,

e. Defines reportable incidents,

f. Provides steps to be taken within the security incident response plan during and after cyberattacks,

g. Provides metrics for measuring the incident response capability within the agency by incident response management function:

   i. Common organizational interfaces: e.g. communications, work coordination

   ii. Protect: e.g. risk assessment, malware protection, vulnerability management

   iii. Detect: e.g. network security monitoring and alerting

   iv. Respond: e.g. incident reporting, incident response, incident analysis

   v. Sustain: e.g. MOUs and contracts, program management, security administration

h. Defines the resources and management support needed to effectively maintain and mature an incident response capability,

i. Be reviewed and approved by designated State or agency officials annually, at a minimum,

j. Be revised as needed to address system/agency changes or problems encountered during plan implementation, execution, or testing,

k. Incident response plan changes must be communicated to identified State and agency officials,

l. Incident response plans must be distributed to State and agency identified incident response personnel,

m. Protect the incident response plan from unauthorized disclosure and modification.

IR-9 - Incident Spillage Response (Optional Control)

This control is optional for LOW and MODERATE risk information systems.

For incident spillage involving FTI, agencies shall refer to IRS 1075 for additional guidance.

IR-10 - Integrated Information Security Analysis Team (Optional Control)

This control is optional for LOW and MODERATE risk information systems.

Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Approved: DocuSigned by: J E Boyd DBF6EB174A72411... 1/30/2018 | 8:25 PM EST

Secretary of Department of Information Technology (DIT)

Policy Approval and Review

Name	Reason	Date