

NORTH CAROLINA DEPARTMENT OF COMMERCE	Policy # MIS-9
	TITLE: Detecting and Reporting Information Security Incidents
Effective Date: July 1, 2005	Administering Authority:
Revisions:	Management Information Systems
Statutory Authority: G.S. §147-33.76(b1)	

The North Carolina Department of Commerce shall adopt and adhere to the following Information Security Incident Detection and Response policy established by the State Chief Information Officer.

Scope: These policies apply to all public agencies, their agents or designees subject to Article 3D of Chapter 147, "State Information Technology Services."

Section 01 Reporting Information Security Incidents

130101 Reporting Information Security Incidents

Purpose: To increase effectiveness in assessing threat levels and detecting patterns or trends in regard to security incidents through proper documentation.

STANDARD

All information technology security incidents must be reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, and must include the information required on the Incident Reporting form,¹ incorporated by reference.

The agency head shall ensure that all information technology security incidents occurring within his/her agency are reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of incident confirmation, as required by N.C.G.S. §147-33.113.²

ISO 17799: 2005 References

13.1.1 Reporting information security events

¹ The Incident Reporting form can be found at <https://incident.its.state.nc.us/> and can be filled out online.

² N.C.G.S. §147-33.82(f).

1301012 Reporting IS Incidents to Outside Authorities

Purpose: To ensure agency awareness of the State's authority to determine when confirmed security incidents should be reported to appropriate third parties.

STANDARD

The ITS Information Security Office, acting on behalf of the State Chief Information Officer, shall determine what, if any, outside authorities need to be contacted in regard to confirmed security incidents in accordance with the Memorandum of Understanding between ITS, the Department of Justice, the State Bureau of Investigation, and the Office of the State Auditor as well as in accordance with federal requirements.

ISO 17799: 2005 References

13.1.1 Reporting information security events

130103 Reporting Information Security Breaches

Purpose: To ensure that all confirmed information security breaches are reported.

STANDARD

State employees and contractors have the responsibility to report security incidents to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, as required by N.C.G.S. §147-33.113 and in accordance with Policy 130101, Reporting Information Security Incidents, and Policy 130102, Reporting Information Security Incidents to Outside Authorities.

ISO 17799: 2005 References

13.1.1 Reporting information security events

130104 Notifying Information Security Weaknesses

Purpose: To reduce information technology security weaknesses.

STANDARD

All agency personnel have the responsibility to report any discovered security weaknesses to their managers. The notification should be made as soon as possible after the weakness is discovered.

ISO 17799: 2005 References

13.1.2 Reporting security weaknesses

130105 Witnessing an Information Security Breach

Purpose: To protect the State's information technology assets.

STANDARD

Individuals who witness a breach in an agency's information technology security shall notify the agency security liaison.

ISO 17799: 2005 References

13.1.1 Reporting information security events

130106 Being Alert for Fraudulent Activities

Purpose: To protect the State's resources.

STANDARD

Suspected fraudulent activity shall be documented and reported to management for appropriate action as soon as possible after it is detected.

ISO 17799: 2005 References

8.2.2 Information security awareness, education, and training

130107 New for 2005

130107 Software Errors and Weaknesses

Purpose: To ensure proper handling of software errors and weaknesses.

STANDARD

Personnel who discover or perceive that there may be a software error or weakness must be report it immediately to management. Management shall notify the responsible individual/organization and perform a risk analysis of the perceived threats.

Individuals who are aware of software errors or weaknesses shall not attempt proof-of-concept actions unless otherwise authorized.

ISO 17799: 2005 References

13.1.2 Reporting security weaknesses

130108 New for 2005

130108 When and How to Notify Authorities

Purpose: To ensure appropriate notification of authorities, regulatory and enforcement agencies about information security incidents.

STANDARD

Agencies shall notify authorities, regulatory and law enforcement agencies about information security incidents in accordance with the State's Incident Management Plan.

If/when authorities, regulatory and/or law enforcement agencies are notified; Agencies shall report the incident to the Incident Management team and/or the Chief Information Security Officer.

ISO 17799: 2005 References

6.1.6 Contact with authorities

Section 02 Investigating Information Security Events

130201 Investigating the Cause and Impact of IS Incidents

Purpose: To protect the State's technology resources by conducting proper investigations.

STANDARD

An investigation into an information security incident must identify its cause, if possible, and appraise its impact on systems and data. Agencies shall contact trained personnel to perform investigations and shall restrict others involved from attempting to gather evidence on their own.

ISO 17799: 2005 References

13.2.2 Learning from information security incidents

130202 Collecting Evidence of an Information Security Breach

Purpose: To protect the State's resources through the proper collection of evidence.

STANDARD

Evidence collected concerning an information security breach shall conform to the legal requirements for collecting such evidence. The collection process shall include a document trail, the chain of custody for items collected, and logs of all evidence-collecting activities.

ISO 17799: 2005 References

13.2.3 Collection of evidence

130203 Recording Information Security Breaches

Purpose: To protect the State's resources through proper reporting of security breaches.

STANDARD

All information technology security breaches must be reported to the ITS Information Security Office, acting on behalf of the State Chief Information Officer, and must include the information required on the Incident Reporting form,³ incorporated by reference.

The agency head shall ensure that all information technology security breaches occurring within his/her agency are reported to ITS, acting on behalf of the State Chief Information Officer, within twenty-four (24) hours of a confirmed breach, as required by N.C.G.S. §147-33.113.⁴

ISO 17799: 2005 References

13.1.1 Reporting information security incidents

130204 Responding to Information Security Incidents

Purpose: To protect the State's resources through proper response to security incidents.

STANDARD

The ITS Information Security Office, acting on behalf of the State Chief Information Officer, shall evaluate the proper response to all information security incidents reported to the agency. ITS shall decide what resources, including law enforcement, are required to best respond to and mitigate the incident.

ISO 17799: 2005 References

13.2.1 Responsibilities and procedures

Section 03 Corrective Activity

130301 Establishing Remedies for Information Security Breaches

Purpose: To help develop rapid resolutions to information security breaches.

STANDARD

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.

³ The Incident Reporting form can be found at <https://incident.its.state.nc.us/> and can be filled out online.

⁴ N.C.G.S. §147-33.82(f).

GUIDELINES

Information recorded in regard to information security breaches should cover the following areas:

- The nature of the breach and the number of systems affected.
- The services that were affected and the resources needed to implement a timely resolution.
- The time at which the breach was discovered and the time at which corrective actions were implemented.
- How the breach was detected and the immediate response after detection.
- The escalation used to resolve the breach.

ISO 17799: 2005 References

13.2.2 Learning from information security incidents

Section 04 Other Information Security Incident Issues

130401 Ensuring the Integrity of IS Incident Investigations

Purpose: To ensure integrity of electronically stored records of information systems incident investigations.

STANDARD

All agencies shall ensure the integrity of information systems incident investigations by having the records of such investigations audited by qualified individuals on a regular basis.

ISO 17799: 2005 References

10.10.2 Monitoring system use
15.3.1 Information systems audit controls
15.3.2 Protection of information systems audit tools

130402 Analyzing IS Incidents Resulting from System Failures

Purpose: To properly analyze information security system failures.

STANDARD

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). Qualified technicians shall perform the investigations, which shall include:

- Checking system logs, application logs, event logs, audit trails and log files.
- Continuing to closely monitor the specified system to establish trends or patterns.
- Researching for known failures resulting from software bugs.

- Contacting appropriate third parties, such as vendor-specific technicians, for assistance.

ISO 17799: 2005 References

13.2.1 Responsibilities and procedures

130403 Breaching Confidentiality

Purpose: To develop a method for identifying and reporting breaches of confidentiality.

STANDARD

Agency staff shall report breaches of confidentiality to appropriate managers within the agency as soon as possible.

Breaches of confidentiality include, but are not limited to, the compromise or improper disclosure of confidential information such as Social Security numbers, medical records, credit card numbers and tax data.

ISO 17799: 2005 References

6.1.5 Confidentiality agreements

6.2.3 Addressing security in third party agreements

130404 Establishing Dual Control/Segregation of Duties

Purpose: To increase the integrity of data while conducting incident investigations.

STANDARD

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

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

ISO 17799: 2005 References

10.1.3 Segregation of duties

13.2.1 Responsibilities and procedures

130405 Using Information Security Incident Check Lists

Purpose: To report information security incidents in a consistent manner.

STANDARD

To ensure consistent reporting of information security incidents, agencies shall use the ITS Incident Reporting form⁵ when reporting such incidents.

ISO 17799: 2005 References

13.2.1 Responsibilities and procedures

130406 Detecting Electronic Eavesdropping and Espionage Activities

The policy recommended by ISO 17799 in this category is not appropriate as a general policy for North Carolina executive branch agencies.

130407 Monitoring Confidentiality of Information Security Incidents

Purpose: To monitor the release of confidential information involving information security incidents.

STANDARD

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 it, such as law enforcement officials, legal counsel and human resources.

ISO 17799: 2005 References

13.2.1 Responsibilities and procedures

130408 New in 2005

130408 Risks in System Usage

Purpose: To monitor systems usage and minimize business risks.

STANDARD

System usage shall be monitored and reviewed for activities that may lead to business risks.

GUIDELINES

Items to monitor may include but not be limited to the following:

- Over utilization of bandwidth.
- Un-authorized login attempts.
- Un-authorized attempts to make changes to system settings.
- Trendy activity, such as to monitor for repeated information security attacks.

⁵ The Incident Reporting form can be found at <https://incident.its.state.nc.us/> and can be filled out online.

