Office of the Governor
State Chief Information Officer

SECURITY

Chapter 6 – Combating Cyber Crime

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

Statutory Authority: N.C.G.S. 147-33.110

Section 01 Combating Cyber Crime

060101 Defending Against Premeditated Cyber Crime Attacks

Purpose: To protect agency networks from a premeditated cyber attack.

STANDARD

Agencies must identify all network access points and verify that the safeguards for the network and individual systems are adequate and operational. These systems include, but are not limited to: wireless access points, network ingress and egress points, and network-attached devices.

Agencies shall deploy controls to ensure that the State's resources do not contribute to outside-party attacks. These controls include but are not limited to:

- Securing interfaces between agency-controlled and non-agency-controlled or public networks.
- Standardizing authentication mechanisms in place for both users and equipment.
- Controlling users' access to information resources.
- Monitoring for anomalies or known signatures via intrusion detection systems and/or intrusion prevention systems.

ISO 17799: 2005 REFERENCE
11.4 Network access control

060102 Minimizing the Impact of Cyber Attacks

Purpose: To minimize the impact of a cyber attack on agency networks.

STANDARD

Agencies shall have security incident management and response plans that address steps to be taken during and after cyber attacks. Agencies shall also

develop contingency plans for the continuation of business processes while under a cyber attack and/or the recovery of data damaged during such an attack. The security incident management and response plans shall be integrated with the business continuity and disaster recovery plans. Both plans shall be developed for use when threats result in loss, corruption, or theft of data or interruption of service due to a cyber attack. These plans shall be developed in accordance with Standard 140102, Assessing the Business Continuity Plan Security Risk, and tested under Standard 140104, Testing the Business Continuity Plan.

ISO 17799: 2005 REFERENCE
14.1.2 Business continuity and risk assessment

060103 Collecting Evidence for Cyber Crime Prosecution

Purpose: To ensure that evidence gathered as a result of cyber crime is admissible as evidence in the prosecution of cyber crime.

STANDARD

In the event of a suspected cyber crime, evidence shall be collected and preserved in a manner that is in accordance with State and federal requirements. In the event of an active cyber crime, management has the authority to decide whether to continue collecting evidence or to lock down the system involved in the suspected crime.

When dealing with a suspected cyber crime, agencies shall:

- Make an image of the system (including volatile memory, if possible) so that original evidence may be preserved.
- 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.
- Take steps to preserve and secure the trail of evidence.
- Report the incident to the ITS Information Security Office within twenty-four (24) hours, as required by law.

ISO 17799: 2005 REFERENCE
13.2.3 Collection of evidence

060104 Defending Against Premeditated Internal Attacks

Purpose: To limit the potential damage caused by internal attacks.

STANDARD

To defend against insider attacks on agency networks and to prevent internal damage, access rights to files shall be controlled to maximize file integrity and to enforce separation of duties.

- Access to files shall be granted only on as required for the performance of job duties..

- Networks that serve different Agencies or departments shall be segregated, and access to those segmented networks shall be established as appropriate through the use of VLANs, routers, firewalls, etc.
- Access badges shall be programmed to allow entry only into assigned places of duty.
- Separation of duties in programming shall be enforced to eliminate trapdoors, software hooks, covert channels, and Trojan code.
- Users' activities on systems shall be monitored to ensure that users are performing only those tasks that are authorized and to provide an appropriate audit trail.

ISO 17799 REFERENCES
10.10.2 Monitoring system use
11.1.1 Access control
11.6.1 Information access restriction

060105 Defending Against Opportunistic Cyber Crime Attacks

Purpose: To reduce the threat of cyber crime attacks.

STANDARD

To protect against opportunistic cyber crime attacks, authentication mechanisms shall be required before access is granted to any agency network resource. Authorization levels shall be reviewed regularly to prevent disclosure of information through unauthorized access.

Vulnerability assessments and penetration tests are tools that can minimize opportunities for cyber crime and are part of a defense-in-depth strategy. When an agency determines that an assessment or test is required, it shall request permission from the State CIO and the State Auditor, as required by N.C.G.S. §147-33.111(c).

ISO 17799 REFERENCE
11.4 Network access control

060106 Safeguarding Against Malicious Denial of Service Attacks

Purpose: To safeguard network resources from denial of service attacks and distributed denial of service attacks.

STANDARD

Each agency shall have the following responsibilities:

- To appropriately secure all hosts that could be a potential target for a denial of service (DoS) or distributed denial of service (DDoS) attack based on the agencies ability to accept the risk for a possible disruption in service from a successful attack.
- To deny all inbound traffic by default, thus limiting the channels of network attacks.
- To periodically scan for bots (software robots) and Trojan horse programs.

- To deploy authentication mechanisms wherever possible.
- To design and implement networks for maximum availability.
- To develop specific plans for responding to DoS and DDoS attacks in the agency incident management plan and the business continuity plan.

ISO 17799: 2005 REFERENCES
9.4 Network access control
13.2.1 Responsibilities and procedures

060107 Defending Against Hackers, Stealth- and Techno-Vandalism

Purpose: To defend the State from cyber-crime-related activities.

STANDARD

To defend the State's assets against hackers, stealth data-gathering software (such as spyware, adware and bots) and techno-vandalism, it is critical to limit the amount of potential exploits within the network infrastructure.

The following duties shall be performed by system administrators or security personnel:

- Periodic scanning for spyware, adware and bots (software robots) with one or more anti-spyware programs that detect these malicious programs and help inoculate the system against infection.
- Denial of all inbound traffic by default through the perimeter defense. Exceptions for traffic essential for daily business must be requested through network security.
- Configuration of public facing systems in accordance with Standard 070103, Configuring E-Commerce Web Sites.
- Provision of security awareness training to personnel on an annual basis that, in part, cautions against downloading software programs from the Internet without appropriate agency approval and outlines the process for addressing virus or other malicious threats to the network. This training should also stress the potential exposure that email attachments presents to the agency and employee.
- Deployment of intrusion detection and/or intrusion prevention systems, as appropriate.

ISO 17799: 2005 REFERENCES
7.1 Responsibility for assets
8.1.1 Roles and responsibilities
8.2.2 Information security awareness, education and training
11.4 Network access control

060108 Handling Hoax Virus Warnings

Purpose: To minimize the threat of hoax virus warnings.

STANDARD

To minimize the threat of hoax virus warnings, incident management procedures shall contain a provision that virus threats are verified before warnings about them are distributed. Appropriately verified warnings shall be distributed by management, agency security administrators, or the ITS Information Security Office through recognized government or verified vendor source, according to State and agency standards, policies and procedures. Agencies shall direct their staffs to follow established standards, policies and procedures and not to forward un-verified virus warnings to others.

ISO 17799: 2005 REFERENCES
6.1.3 Allocation of information security responsibilities
10.4.1 Controls against malicious code

060109 Defending Against Virus Attacks

Purpose: To minimize virus attacks.

STANDARD

All files downloaded to the State network might potentially harbor computer viruses, Trojan horses, worms or other destructive programs (collectively, “virus” or “viruses”); therefore, all downloaded files must be scanned for such viruses. Virus detection programs and practices shall be implemented throughout agencies. Training must take place to ensure that all computer users know and understand safe computing practices. All agencies shall be responsible for ensuring that they have current software on their network to prevent the introduction or propagation of computer viruses.

Agencies shall select and use virus prevention and mitigation standards and best practices as appropriate.

Virus controls, procedures, education and training shall include the following:

- Information on:
  - Use of antivirus software.
  - Performing frequent backups on data files.
  - Use of write-protected program media, such as diskettes or CD-ROMs.
  - Validating the source of software before installing it.
  - Scanning for viruses on files that are downloaded from the Internet or any other outside source.
  - Scanning for viruses on all diskettes, CDs or other media brought from home or any other outside source.
  - Requirements that users first obtain management approval before directly adding any software to the system, whether from public software repositories, other systems or their home systems.

ISO 17799 REFERENCE
10.4.1 Controls against malicious code

060110 Responding to Virus[1] Incidents

Purpose: To establish an effective response to virus incidents.

STANDARD

To mitigate the propagation of viruses and to protect agency networks, each agency shall develop a cyber security incident management plan for controlling the potential negative consequences of an incident.

Agency plans shall include:

- Incident response team members and contact information.
- Procedures for detecting, responding to and recovering from virus incidents.
- Procedures for notifying the agency and the ITS Information Security Office.
- Staff training.
- Testing of the plan.

Each agency shall collect and preserve evidence of information technology security incidents in accordance with Standard 060103, Collecting Evidence for Cyber Crime Prosecution. Documentation of any incident shall be thoroughly performed for later review.

An agency's incident management plan shall include the following elements:

- Verification of a virus threat, to rule out possibility of hoax, before notification of the threat is broadcast.
- The identity of personnel responsible for mitigation of virus threats.
- Internal escalation procedures and severity levels.
- Processes to identify, contain, eradicate, and recover from virus events.
- A contact list of antivirus software vendors.
- Reporting to the ITS Information Security Office all virus outbreaks that have extended beyond a single PC, as required by N.C.G.S. §147-33.113(a)(1).
- Review by staff, after each information technology security incident, of the lessons learned from the incident, with any necessary changes subsequently made to the agency incident management plan.

ISO 17799: 2005 REFERENCES

10.4.1	Controls against malicious code
13.1.1	Reporting information security events
13.2.1	Responsibilities and procedures

[1] For purposes of these standards, the term *virus* covers viruses, Trojan horses, worms and other destructive and malicious code.

060111 Installing Virus Scanning Software

Purpose: To ensure the proper installation of appropriate antivirus software.

STANDARD

Agencies shall install robust antivirus software on all LAN servers and workstations, including those used for remote access to the State network. In addition, system antivirus software, including virus signature files, shall be promptly updated as updates are released by the software vendor.

System configuration management shall include:

- Maintenance of good backups of critical data and programs.
- Periodic review of overall controls to determine weaknesses.
- Prohibition of network connections to outside organizations without a mutual review of security practices.
- Limiting use of software to that which can be verified to be free of harmful code or other destructive aspects.
  - Complete information about the software shall be maintained, such as the vendor address and telephone number, the license number and version, and update information.
  - Configuration reports shall be maintained of all installed software, including the operating system. This information will be necessary if the software must be reinstalled later.
  - Software programs shall be reinstalled only from validated media.
  - Software shall be stored in a secure, tamper-proof location.
- System and application bug fixes or patches shall be accepted only from highly reliable sources, such as the software vendor.
- Patches shall be accepted from trusted and verified sources.

ISO 17799 REFERENCE
10.4.1 Controls against malicious code

HISTORY

Approved by State CIO: March 22, 2006
Original Issue Date: March 22, 2006
Subsequent History:

Standard Number	Version	Date	Change/Description

Old Security Policy/Standard	New Standard Numbers
Incident Management Policy	060102 – Minimizing the Impact of Cyber Attacks
	060103 – Collecting Evidence for Cyber Crime Prosecution
	060108 – Handing Hoax Virus Warnings
	060110 – Responding to Virus Incidents
	120401 – Recording Evidence of Information Security Incidents
	Chapter 13 – Detecting and Responding to IS Incidents