NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Statewide Organizational Threat Management Policy

Statewide IT Policy

Version 1.0

March 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
February, 2026	1.0	New	Standard Creation	Martha K. Wewer

Document Details

Department Name	Office of Privacy and Data Protection
Owner	Martha K. Wewer, Statewide Chief Privacy Officer
Title	Statewide Organizational Threat Management Policy
Publication Date	March, 2026
Next Release	Annual Review
Document Type	Policy
Version	1.0

Contents

Purpose

The purpose of this Organizational Threat Management Policy is to establish guidelines to prevent, detect, and respond to internal security threats to the state of North Carolina intentionally perpetrated to cause harm to the organization through education, awareness, and proactive, preventative measures while maintaining staff privacy and confidentiality. This policy aims to protect the organization's assets, including sensitive information and IT infrastructure, from threats posed by individuals within the organization and direct agencies to establish an Organizational Threat Team.

Owner

Statewide Office of Privacy and Data Protection

Scope

This policy applies to all employees, contractors, interns, and any individuals who have access to State Information Systems and State Data, both electronic and paper. It covers all forms of threat that can arise from staff, whether intentional or unintentional.

Policy

Pursuant to N.C.G.S. 143B-1376(a) and the Security Awareness and Training Policy (AT-2(2)), the State of North Carolina recognizes that threats from within an organization – sometimes called "insider" threats – can be as damaging as external threats. As such, state agencies must be committed to:

- Identifying potential organizational threats
- Providing training on recognizing them and how to report concerns
- Taking preventative measures to prevent and avoid potential threats
- Responding effectively and swiftly when a threat is identified

An "organizational" threat is an individual with authorized access who has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. Additionally, a threat to an organization can also come from employees, former employees, contractors, or anyone else who has or had access to the organization's assets.

Such threats include, but are not limited to, theft of intellectual property, sabotage of IT systems, and unauthorized disclosure of Confidential Information or Restricted Information (see Statewide Data Classification and Handling Policy or See the Statewide Glossary of IT Terms. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities.

Identifying Types of Organizational Threats

Organizational threats fall into two categories: unintentional and intentional.

Unintentional Threats

Unintentional threats are those that can cause harm to the State as a result of negligent or accidental behavior of staff.

- Examples of negligence resulting in harm are ignoring messages to install updates or security patches or losing a portable storage device containing State Data.

- Examples of accidental acts resulting in harm to the State are sending State Data via email to the wrong person, failing to encrypt a media or thumb drive containing sensitive information or improperly disposing of State Data.

Events such as these should be reported to the state agency privacy and/or security contact or in accordance with the state agency's Incident Response plan.

Intentional Threats

Intentional threats are actions taken to harm an organization or an individual within the organization for personal benefit, to act on a personal grievance or under duress or influence by an outside entity.

Examples of intentional threats include leaking sensitive information, threatening staff, stealing proprietary data or intellectual property, or sabotaging systems or equipment. Espionage, sabotage, theft, physical threats, and cyberthreats are all examples of intentional organizational threats.

Detection

Agencies should establish appropriate measures to detect organizational threats. For example:

- Monitoring systems and behaviors for indicators of insider risk
- Managing user access based on least privilege and need-to-know principles
- Conducting background checks and periodic re-screening, where appropriate
- Maintaining sensitive information in secure, access-restricted areas
- Enforcing a "clean desk" policy

Training

Staff will complete annual Organizational Threat Awareness training to recognize signs of intentional threats from within the organization.

Reporting and Response

The State of North Carolina is committed to maintaining a secure environment and reducing the risk of insider threats by promoting a culture of security awareness and accountability while protecting employee privacy and safety.

Each Agency must develop an Organizational Threat Team. It is recommended that Agency Organizational Threat Teams include security, privacy, General Counsel, and Human Resources.

Should you see suspicious activity, please report the behavior promptly and confidentially using the Statewide Cybersecurity Incident Report Form or to Enterprise Security Risk Management Office (ESRMO)

If a credible organizational threat is reported, follow the ESRMO Incident Response Policy and Procedure. The Agency should begin an investigation, which will include interviews, user activity monitoring, revocation or suspension of access privileges (particularly privileged or admin account privileges), and suspension of badge privileges consistent with the Agency's own established procedure

A report containing the findings and remediation recommendations from ESRMO will be presented to the Agency Chief Information Officer (CIO).

Roles and Responsibilities

- State Chief Information Officer (CIO): Reviews response and remediation recommendations.
- State Chief Information Security Officer (CISO): Investigates and coordinates monitoring, access and log reviews and executes response; leads ESRMO.
- Agency CISO: works with Agency CIO to investigate, monitor and remediate.
- Agency CIO: Investigates and coordinates monitoring, access and log review; executes response.
- Agency Human Resources: Supports investigations, coordinates employee interviews.
- Agency Office of General Counsel: Provides legal advice and coordinates with law enforcement, if necessary.
- Statewide Chief Privacy Officer (CPO): Identifies sensitivity of the data; provides subject matter expertise on privacy laws and regulations.
- Agency Security Liaison: works with Agency CIO and CISO to coordinate with State CISO and ESRMO regarding response and remediation.
- Agency Privacy Liaison: works with State CPO regarding data sensitivity.

Regulations and Applicable Laws

- N.C.G.S. 143B-1376(a)

Enforcement

Violations of this policy may result in disciplinary action in accordance with N.C.G.S. 126-35(a) and 25 NCAC 01J .0604 for Career State employees (Covered Employees). Violations may also be reported to other State entities in accordance with applicable North Carolina State Laws, including but not limited to N.C.G.S. 143B-1208.6[1] and N.C.G.S. 147-64.6B.[2]

State employees with a Statutorily Exempt position are not subject to Chapter 126, the State Human Resources Act. Pursuant to N.C.G.S. 143B-10(c), all employees within a principal State department shall be under the supervision, direction, and control of the head of that department. Therefore, the head of each principal State department may establish or abolish positions and take disciplinary action in accordance with applicable State laws and internal policies. Violations may be reported to other State entities in accordance with applicable North Carolina State Laws, including but not limited to N.C.G.S. 143B-1208.6 and N.C.G.S. 147-64.6B.

Parties enforcing this policy Enterprise Security and Risk Management Office, the Office of Privacy and Data Protection, Human Resources and the Office of the General Counsel.

Policy Review Cycle

The Organizational Threat Management Policy will undergo a periodic review at annual intervals, or as changes are required. Updates to the policy will be determined based upon the nature of the policy and requirements driven by need.

---

[1] N.C.G.S. 143B-1208.6 requires **department heads to report possible violations of criminal statutes involving misuse of State property to State Bureau of Investigation.**

[2] N.C.G.S. 147-64.6B (state auditor) is not mandatory but allows reports of allegations of improper governmental activities of State agencies and State employees within the scope of authority set forth in N.C.G.S. 147-64.6, including misappropriation, mismanagement, or waste of State resources, fraud, violations of State or Federal law, rule or regulation by State agencies or State employees administering State or federal programs, and substantial and specific danger to the public health and safety.

Any identified changes, or outdated information within the policy will be addressed promptly. This may involve revisions, additions, or removals as needed to ensure that policies remain current and relevant.

The following roles provide leadership and management over this policy in accordance with the NCDIT Policy Management Policy:

- State Chief Information Security Officer
- State Chief Privacy Officer
- Director of Human Resources
- Office of the General Counsel

Definitions

Espionage

Espionage is the covert or illicit practice of spying on a foreign government, organization, entity, or person to obtain Confidential Information or Restricted information for military, political, strategic, or financial advantage.

- **Economic Espionage** is the covert practice of obtaining trade secrets from a foreign nation (e.g., all forms and types of financial, business, scientific, technical, economic, or engineering information and methods, techniques, processes, procedures, programs, or codes for manufacturing).
- **Government Espionage** is covert intelligence-gathering activities by one government against another to obtain political or military advantage. It can also include government(s) spying on corporate entities such as aeronautics firms, consulting firms, think tanks, or munition companies. Government espionage is also referred to as intelligence gathering.
- **Criminal Espionage** involves an individual betraying U.S. government secrets to foreign nations.

Sabotage

Sabotage is the deliberate actions to harm an organization's physical or virtual infrastructure, including noncompliance with maintenance or IT procedures, contaminating clean spaces, physically damaging facilities, or deleting code to prevent regular operations.

- **Physical Sabotage** is taking deliberate actions aimed at harming an organization's physical infrastructure (e.g., facilities or equipment).
- **Virtual Sabotage** is taking malicious actions through technical means to disrupt or stop an organization's normal business operations.

Theft

Theft is the act of stealing, whether a physical item such as money or an intangible item such as data, trade secrets, or intellectual property.

- **Financial Crime** is the unauthorized taking or illicit use of a person's, business', or organization's money or property with the intent to benefit from it.
- **Intellectual Property Theft** is the theft or robbery of an individual's or organization's ideas, inventions, or creative expressions, including trade secrets and proprietary products, even if the concepts or items being stolen originated from the thief.

Cyberthreats

Cyberthreats include theft, espionage, violence, and sabotage of anything related to technology, virtual reality, computers, devices, or the internet.

References

- Statewide Information Technology Glossary
- Statewide Information Security Manual
- Statewide Data Classification and Handling Manual