NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Privacy & Data Protection Policy

Statewide IT Policy

Version 1.0

August 10, 2026

Document Information

Revision History

Date	Version	New or Revised Requirement	Description	Author
MM DD, 20XX	1.0	New	Policy Creation	

Document Details

Department Name	Privacy and Data Protection Policy
Owner	Office of Privacy and Data Protection
Title	Statewide Chief Privacy Officer
Publication Date	
Next Release	
Document Type	
Document Number	
Version	1.0

Purpose

North Carolina's Office of Privacy and Data Protection (OPDP) is tasked by the State Chief Information Officer and Secretary of the N.C. Department of Information Technology (NCDIT) with protecting state data. OPDP is committed to protecting the privacy rights of all North Carolinians, as required by N.C.G.S. 143B-1376 – Statewide Security and Privacy Standards.

OPDP enforces data minimization, purpose limitation, appropriate data classification, responsible use, and secure handling throughout the full lifecycle of state data. The office also implements a statewide privacy program that embeds Privacy by Design and Privacy by Default into state operations. This policy defines the elements of the statewide privacy program, assigns agency obligations, and establishes a unified governance framework for protecting state data.

Owner

N.C. Department of Information Technology – Office of Privacy & Data Protection

Scope

This policy applies to state agencies, as defined in N.C.G.S. 143B-1320, that are subject to Article 15 of Chapter 143B of the North Carolina General Statutes, unless otherwise exempt or provided by law.

Policy

Governance & Accountability

Pursuant to N.C.G.S. 143B-1376 – Statewide Security and Privacy Standards, the State Chief Information Officer (CIO) is responsible for the security and privacy of all state information technology systems and associated data.

The State CIO oversees information technology security for all executive branch agencies and is responsible for creating a statewide standard for IT security and privacy. This statewide standard is designed to ensure that the state's distributed IT assets are functional, secure, and interoperable. It covers areas such as data classification and management, as well as communications and encryption technologies.

The Office of Privacy and Data Protection (OPDP) is the enterprise division within the N.C. Department of Information Technology that the State CIO has tasked with establishing privacy standards across the state.

State agencies that are subject to the statewide security and privacy standards (established under N.C.G.S. 143B, Article 15) are required to maintain documented privacy governance structures, which include designated privacy roles, responsibilities, and reporting lines. Agencies must also designate system owners and data stewards who are responsible for privacy requirements throughout the data lifecycle, as described in the Statewide Data Classification and Handling Policy.

OPDP establishes and oversees statewide privacy governance and conducts periodic reviews to ensure adherence to statewide standards.

Agencies may use this policy and associated procedures as a baseline measure for their own privacy programs.

The statewide privacy program sets forth privacy controls – in coordination with the Statewide Information Security Manual (SISM) – which are the minimum standards to which all agencies must adhere. Agencies may develop internal policies and procedures that build upon OPDP's statewide policies. These policies and procedures, however, must remain consistent with statewide privacy standards. They may not conflict with or be less stringent than those standards.

In addition, each state agency shall develop, document, and maintain a privacy risk management strategy that prioritizes privacy risks according to the agency's specific mission, data types, and data use and processing activities. This strategy should be reviewed and updated annually and be made available to OPDP upon request.

Privacy Incident Response

As a critical function of governance and accountability, OPDP shall maintain a formal incident response capability to manage events in which Personal Information may be compromised.

A **Privacy Incident**, as defined in the Statewide Privacy Incident Response Procedure, means a violation of privacy policy or procedure. This includes but is not limited to:

- Inappropriate data aggregation
- Unauthorized access and/or acquisition
- Use for an unauthorized purpose (purpose violation)
- Any other event that compromises the confidentiality, integrity, or availability of Personal Information

All incident response activities shall be conducted in accordance with the Statewide Privacy Incident Response Procedure (in compliance with NIST SP 800-61r3).

The incident response lifecycle shall be comprised of four phases:

- **Preparation:** To establish proactive capabilities
- **Detection and Analysis:** To identify and validate incidents
- **Containment, Eradication, and Recovery:** To limit impact and restore operations
- **Post-Incident Activity:** To analyze outcomes and implement improvements.

Each state agency shall have a dedicated Incident Response Team or designated personnel (collectively referred to in this policy as "Incident Response Team") to manage and coordinate privacy incident response activities.

All personnel shall immediately report suspected privacy incidents to the Incident Response Team.

The Incident Response Team shall be responsible for analyzing, containing, and eradicating confirmed incidents. It should collaborate closely with the agency's designated Privacy Officer or Privacy Point of Contact to ensure all actions are compliant with applicable laws, regulations, and policies. The Incident Response Team shall also manage all required notifications to affected individuals or regulatory authorities, as applicable.

Privacy Risk Assessment Requirements

Privacy Threshold Analysis

State agencies are required to complete a Privacy Threshold Analysis (PTA) for any new project or system or when a project or system undergoes a material change that impacts the collection, use, disclosure, storage, or processing of state data. This includes but is not limited to:

- Procurement of new software
- Development of a new or updated agency program that involves the processing of state data

Privacy Impact Assessment

If the PTA indicates that Personal Information is collected, used, or maintained, agencies must complete a Privacy Impact Assessment (PIA) – a tool used to identify, assess, and mitigate privacy risks.

The PIA process is managed by OPDP.

AI-Use Case Risk Profile

For tools or systems using artificial intelligence (AI), state agencies should be prepared, if requested, to submit a completed AI-Use Case Risk Profile with the PTA/PIA.

Data Risk Register

To ensure risk management is a continuous practice, each agency must also maintain a Data Risk Register for any system processing Confidential or Restricted data. The register must be reviewed and updated at least annually.

For guidance on creating and maintaining a Data Risk Register, please contact the Office of Privacy and Data Protection at opdp@nc.gov.

Privacy Points of Contact

Each state agency shall establish a Privacy Point of Contact (see section below) to oversee the PTA completion process.

Moreover, the Privacy Officer or Privacy Point of Contact must be engaged to review the information in the PTA to ensure it is complete and accurate. This includes reviewing the vendor's privacy policy, if applicable.

For more information regarding the PTA/PIA process, please see the statewide procedure on PTAs and PIAs.

Privacy and Data Analytics

Agencies conducting data analytics or designing systems that process Restricted data must have a policy or procedure that documents the implementation of De-Identification, Differential Privacy, Pseudonymization, or Format-Preserving Encryption as part of the system design phase. (Refer to NIST SP 800-226 for additional information.).

This helps move Privacy by Design from being just a principle to an enforceable technical requirement.

In addition, all system configurations must default to the most restrictive privacy settings to implement Privacy by Default at the architectural level. Any data intended for public classification through de-identification must follow the rigorous procedures defined in the Statewide Data Classification and Handling Policy.

To ensure a defense-in-depth approach, all technical controls shall also align with the NIST Privacy Framework and the NIST SP 800-53 Privacy Control Families, ensuring that privacy is a foundational and non-negotiable component of the system architecture. For guidance on required technical controls under NIST SP 800-53, please reach out to DITPrivacy@nc.gov

Privacy Points of Contact

Agencies must have a designated Privacy Point of Contact to help ensure accountability and efficient privacy communications both within the agency and with OPDP.

The CIO of any agency without a Privacy Officer must appoint at least one person to serve in the role.

The designated Privacy Point of Contact serves as the agency's privacy liaison to OPDP and is also responsible for:

- Assisting with any internal privacy matters, including reviewing new projects, programs, systems, and services
- Ensuring that required privacy training is completed every two months
- Attending OPDP's monthly privacy meetings and notifying any internal stakeholders of any privacy concerns or information discussed in that meeting
- Executing the agency's formal Privacy Incident Response Plan upon discovery of a suspected incident and ensuring timely reporting to OPDP
- Ensuring all agency data practices adhere to the mandatory controls specified in the Statewide Data Classification and Handling Policy

Resources dedicated to privacy will vary between agencies based on the size of the agency as well as the scope and scale of Personal Information the agency processes. The Privacy Point of Contact must possess the requisite training and knowledge, such as additional privacy training and industry certification.

OPDP maintains and updates annually a list of Privacy Point of Contacts. If you have questions regarding who this is or need to update your agency's contact, please send an email to OPDP@nc.gov

Privacy Policies & Procedures – Statewide Level

OPDP maintains up-to-date statewide privacy documentation, which includes:

- Data inventories
- Dataflow maps
- Policies and procedures
- Statewide templates

OPDP evaluates and updates documentation at least once a year or whenever systems change to ensure they align with evolving laws and industry best practices.

OPDP will provide guidance to state agencies on compliance with statewide policies and procedures, data inventories, and data flow maps when requested and commits to respond to requests within the agreed upon Service Level Agreement (SLA) or Memorandum of Understanding (MOU).

Privacy Policies & Procedures – Agency Level

State agencies must maintain a documented privacy program that includes:

- Policies and procedures
- Data flow documentation
- Privacy training
- Vendor oversight
- Risk assessments
- Website privacy policies

- Compliance monitoring

Vendor Oversight

Agencies shall agree to use the Statewide IT Terms and Conditions or execute a formal Data Sharing Agreement (DSA) or Privacy Addendum for all third-party contracts involving state data. This agreement must include a right to audit clause that enables OPDP or the agency to verify vendor compliance.

Policy Reviews & Updates

Each state agency must review and update its privacy practices annually. Agencies may develop internal policies and procedures that build upon OPDP's statewide policies. Such policies and procedures, however, may not conflict with or be less stringent than statewide requirements.

Website Privacy Policies

Websites maintained at the agency level must have a privacy policy that describes the data collected by the website for the agency. Those privacy policies should be reviewed and updated annually.

A privacy policy template is available to agencies upon request.

Privacy Program Measurement

OPDP shall enforce a formal assessment process to ensure state agency compliance and measure program maturity through a standardized Privacy Scorecard assessment. The scorecard provides a quantitative measurement of each agency's adherence to the privacy controls and obligations set forth in this policy, the Statewide Data Classification and Handling Policy, and the Statewide Information Security Manual (SISM).

OPDP will provide agencies the Privacy Scorecard for completion on an annual basis.

Upon completion of the Privacy Scorecard, state agencies are required to develop a formal Corrective Action Plan to address any identified deficiencies or areas of low maturity. This plan must be documented and submitted to OPDP for review.

The annual review of each agency's privacy program will, in turn, evaluate the progress made against this Corrective Action Plan, thereby creating a continuous cycle of measurement, remediation, and accountability.

At a minimum, the Corrective Action Plan must formally document the following for each finding:

1. **Specific Deficiency:** A clear identification of the control or policy requirement that is not being met, as cited in the Privacy Scorecard
2. **Remedial Actions:** A detailed description of the specific actions, process changes, or technology implementations the agency will undertake to address the deficiency
3. **Responsible Parties:** The designation of the specific office, role, or individual responsible for overseeing the implementation of the remedial actions
4. **Timeline for Completion:** A realistic and committed timeline with key milestones for the completion of all required actions

OPDP shall monitor agency progress against the approved CAP. The successful implementation of the Corrective Action Plan will be a primary factor in the subsequent annual review of the agency's privacy program, thereby creating a continuous and enforceable cycle of measurement, remediation, and accountability.

Retention & Disposition of State Data

State agencies must dispose of Personal Information in a manner consistent with the Statewide Information Security Manual, the Statewide Data Classification and Handling Policy, applicable laws and regulations, and the agency's own privacy policies.

Disposal should only occur after all record retention requirements have been met and the information is no longer needed for its original purpose or to comply with other legal requirements.

These legal requirements may include but are not limited to the terms of executed data sharing agreements (DUAs), MOUs, MOAs, and applicable state and federal requirements.

The state's Data Retention Guidelines are available on the State Archives of North Carolina website.

Privacy Training

Agencies must ensure all staff receive sufficient privacy awareness training related to their roles and responsibilities and the Personal Information they have access to.

At minimum, agencies must ensure their employees and contractors complete the statewide LMS privacy training that OPDP provides every two months.

OPDP periodically offers additional privacy training opportunities to Privacy Officers and Privacy Points of Contact, including agency-specific training that must be completed annually.

Because each state agency handles different data, agencies are encouraged to create their own privacy training that is applicable to their privacy needs. Upon request, OPDP can review and assist with providing training guidance.

Privacy's Role in Artificial Intelligence

As state agencies adopt AI technologies – both through internal development and procurement from third-party vendors –they must safeguard privacy and protect state data.

Regardless of whether an AI system is developed in-house or acquired externally, agencies must ensure it adheres to Privacy by Design principles, the PTA/PIA, procedure, the Agency AI Starter Pack, and the Statewide Data Classification and Handling Policy. This includes assessing vendors' data handling practices, ensuring transparency in how AI processes Personal Information, and embedding privacy protections from the outset.

Agencies shall ensure that third-party vendors meet the state's stringent privacy standards. By conducting thorough privacy and artificial intelligence impact assessments, they can better identify risks, take steps to mitigate those risks, maintain public trust, and ensure compliance with state and federal privacy laws and policies. (For additional information on conducting an Artificial Intelligence Impact Assessment, see the statewide policy on PTAs and PIAs.)

In addition, users must adhere to the North Carolina State Government Responsible Use of Artificial Intelligence Framework.

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.

Policy Review Cycle

The Privacy and Data Protection Policy will be reviewed annually, or as changes are required. Updates to the policy will be determined based upon the nature of the policy and requirements driven by need.

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.

- State Chief Privacy Officer, Office of Privacy and Data Protection
- State Chief Information Security Officer, Enterprise Security and Risk Management Office

State Privacy Laws & Principles

Personal Information (PI)

Under North Carolina's Identity Theft Protection Act (Chapter 75, Article 2A, N.C.G.S. 7561(10)), "personal information" is defined as follows:

> A **person's first name or first initial and last name** in **combination with any** of the following identifying information found in G.S. 14-113.20(b).

Identifying Information

Under N.C.G.S. 14-113.20(b), the term "identifying information" includes the following:

1. Social Security or employer taxpayer identification numbers
2. Driver's license, state identification card, or passport numbers
3. Checking account numbers
4. Credit card numbers
5. Saving account numbers
6. Debit card numbers
7. Personal identification (PIN) Code as defined in N.C.G.S. 14-113.8(6)
8. Electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names
9. Digital signatures
10. Any other numbers or information that can be used to access a person's financial resources
11. Biometric data
12. Fingerprints
13. Passwords
14. Parents legal surname prior to marriage

To review and learn more about North Carolina privacy statutes please visit: Privacy Laws, Policies & Guidance | NCDIT.