NCDIT NORTH CAROLINA DEPARTMENT OF INFORMATION TECHNOLOGY

Roy Cooper
Governor

James A. Weaver
Secretary and State Chief Information Officer

Memorandum

To: Council of State, Agency CIOs, Privacy Points of Contact, and Security Liaisons

From: Cherie L. Givens, Chief Privacy Officer
NC Department of Information Technology

Subject: **Adoption of the Fair Information Practice Principles**

Date: May 19, 2022

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 manages all executive branch information technology security and shall establish a statewide standard for information technology security and privacy 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.

In support of this duty, the N.C. Department of Information Technology's (NCDIT) Office of Privacy and Data Protection (OPDP) adopted the Fair Information Practice Principles (FIPPs) in January 2022. The FIPPs provide guidance to agencies on reducing privacy risks and supporting the creation of reliable records to inform decision-making. The FIPPs are widely accepted in the United States and around the world as a general framework for privacy.[1] They are reflected in policies and guidance adopted by NCDIT. These principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.

The eight guiding principles are:

1. **Transparency:** The organization should be transparent and provide notice to the individual regarding its collection, use, dissemination and maintenance of personally identifiable information (PII).
2. **Individual Participation:** Consent should be sought from the individual for the collection, use, dissemination and maintenance of PII. A mechanism should also be provided for appropriate access, correction and redress regarding the organization's use of PII.
3. **Purpose Specification:** The organization should specifically articulate the authority that permits the collection of PII and the purpose(s) for which the PII is intended to be used.
4. **Data Minimization:** The organization should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as it is necessary to fulfill those purpose(s).
5. **Use Limitation:** The organization should use PII solely for the purpose(s) specified in the notice. Sharing PII outside of the organization should be for a purpose compatible with the purpose(s) for which the PII was collected.
6. **Data Quality and Integrity:** The organization, to the extent practicable, should ensure that PII is accurate, relevant, timely and complete.

7. **Security:** The organization should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.
8. **Accountability and Auditing:** The organization should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements.[2]

If you have any questions about the adoption of the FIPPs, please contact Chief Privacy Officer Cherie Givens at cherie.givens@nc.gov or 919-754-6578.

Cherie L. Givens Digitally signed by Cherie L. Givens
Date: 2022.05.19 15:29:08 -04'00'

CHERIE L. GIVENS, JD, PhD, CIPP

[1] NIST Glossary Terms, https://csrc.nist.gov/glossary/term/FIPPs, accessed April 22, 2022.
[2] Adapted from Teufel, H. (2008, December 29) The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security [Memorandum]. Department of Homeland Security.