NC DEPARTMENT of COMMERCE
COMMUNITY REVITALIZATION

Personally Identifiable Information (PII) Policy

North Carolina Department of Commerce

Division of Community Revitalization

Version 1.0 – March 11, 2026

Revision History

Version	Date	Description
1.0	March 11, 2026	Initial version

Table of Contents

Overview

The North Carolina Department of Commerce's Division of Community Revitalization (DCR) is committed to protecting the privacy of individuals' information in accordance with federal and state privacy-related laws, guidance, and best practices. This Personally Identifiable Information (PII) Policy is intended to guide DCR's and DCR's partners' collection, use, maintenance, and dissemination of such information in the implementation of Community Development Block Grant Disaster Recovery (CDBG-DR) programs. It applies to DCR staff, contractors, subrecipients, and any other individual or entity as set out herein.

Definitions

Personally Identifiable Information (PII)

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

Sensitive Personally Identifiable Information (SPII)

Sensitive PII is PII that when lost, compromised, or disclosed could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. In determining what PII is sensitive, the context in which the information is used must be considered. Examples of SPII include social security numbers, driver's license numbers, medical records, financial account numbers, and PII combined with additional sensitive information, such as whether the individual is applying for or receiving public assistance. In order to protect PII that may be combined with sensitive information, this Policy will refer to privacy information as PII throughout.

Protection of PII

As part of its authorized activities, DCR collects and retains PII relating to program staff, contractors, subrecipients, and applicants for assistance. To ensure compliance with policies and regulations

regarding the protection of PII, DCR will take all steps necessary to ensure the privacy and protection of such information from unauthorized disclosure. Specifically, DCR will:

1. Limit the collection of PII to only the PII needed for program purposes.
2. Manage access to PII, including:
    a. Only sharing or discussing PII with those who are authorized to know for official work purposes and only to the extent necessary to perform authorized job functions and official duties within DCR;
    b. Only distributing or releasing PII to others if the release is authorized as set out in this Policy or as required by law; and
    c. Avoid discussing sensitive PII where unauthorized individuals may overhear the conversation.
3. Protect hard copy files containing PII, including:
    a. Clearly labeling all files containing PII;
    b. Locking up all files containing PII in secured file cabinets and not leaving PII in open areas unattended;
    c. Shredding or placing in a confidential shredding container any documents containing PII, if those documents are also appropriately saved digitally in accordance with record retention requirements; and
    d. Not leaving PII documents on a printer where unauthorized individuals may have access to the information and requiring the use of a secure printing process with a PIN or an ID badge so that documents are not released from the printer until the person printing is present.
4. Protect electronic files containing PII, including:
    a. Following applicable North Carolina statewide information security requirements, including the NCDIT Statewide Information Security Manual (SISM) and Enterprise Risk and Security Management Office (ESRMO) directives;
    b. Storing PII on systems of record that meet the state's security standards and ensuring third parties and providers of external system services comply with statewide security and privacy requirements: Document Approval and Review Information

c. Protecting digital copies of files containing PII. Protections may include encryption, enhanced authentication mechanisms such as two-factor authentication, and limitations to the number of people allowed access to the files;
d. Not placing PII on a thumb drive or a removeable media device;
e. Ensuring PII is not stored where unauthorized individuals can access it, such as on shared drives, multi-access calendars, the intranet, or the internet;
f. Training staff on cybersecurity in compliance with the State's Security Awareness and Training Policy: Security Awareness and Training Policy;
g. Not entering PII into any generative AI system, automated processing tool, or publicly available AI tool unless explicitly authorized and determined to be compliant with applicable statewide policy and security controls.

5. Have DCR staff, contractors, subrecipients, and any other individuals with access to program PII sign the Acknowledgment Form in Appendix A of this Policy.
6. Follow applicable state and federal record retention requirements and disposition procedures.

DCR will comply with the Statewide Data Classification and Handling Policy for all program data, including PII.

DCR may receive data from FEMA in order to make Duplication of Benefits determinations for applicants to DCR's programs. DCR must protect such information in the same manner that the Privacy Act requires FEMA to protect it and may not further disclose the information to other entities or use it for purposes other than providing additional disaster assistance to individuals and households. Data that DCR receives from other federal agencies will be protected in the manner required by those agencies and applicable federal law.

Protecting the Confidentiality of Applicants for Public Assistance

The data collected from applicants for CDBG-DR assistance contains PII, and unauthorized disclosure of such PII may result in civil and criminal penalties. DCR does not disclose the names or other information concerning persons applying for or receiving public assistance without their consent except in the course

of performing its official duties. PII of persons applying for public assistance may only be used for the following limited purposes:

1. DCR and agents acting on its behalf may use PII throughout the award determination and closeout process to determine eligibility, ensure compliance with program requirements, reduce errors, and mitigate fraud, waste, and abuse.
2. DCR may disclose PII of an applicant to those with duly authorized power of attorney for the applicant or for whom the applicant has provided written consent to do so.
3. DCR may disclose PII to auditors performing a financial or programmatic audit.
4. DCR may disclose PII when required by federal or state laws and regulations.
5. DCR may disclose PII to relevant law enforcement agencies to investigate allegations of fraud.
6. DCR may disclose limited PII to third parties to make Duplication of Benefits (DOB) determinations, seek necessary permits and utilities connections, facilitate or provide Temporary Relocation Assistance, and meet specific unmet needs related to the purpose for which the PII was collected.

DCR may require third parties receiving applicant data to enter into a data sharing agreement and agree to follow this PII Policy. Third parties requesting PII from DCR must identify the purpose for which the data will be used and how that will further the goals of DCR's CDBG-DR programs. DCR will not release applicants' PII to third parties except as described in this Policy or with written consent from the applicant(s). DCR will obtain applicant consent before sharing PII related to that applicant for media or outreach purposes.

Contractor and Subrecipient Responsibilities

DCR's subrecipients and contractors collect and retain PII relating to staff, applicants for direct assistance, and applicants for rental housing. These subrecipients and contractors must adopt and comply with this PII Policy and affirm that:

- Access to program PII is restricted to a limited number of staff;
- Relevant staff have reviewed this PII Policy and signed the Acknowledgement Form in Appendix A;
- Staff have been instructed on how to protect hard copy and electronic PII and how to report a security breach incident, in accordance with this Policy; and

- The subrecipient or contractor has secure systems for protecting PII stored electronically.

Contractors and subrecipients may not enter into a third-party data sharing agreement to share program PII without DCR's consent.

To the extent that any provision of this Policy conflicts with the terms of the contract between DCR and the subrecipient or contractor, the contract shall govern and the conflicting provision of this Policy shall be deemed modified to the extent necessary to conform with the contract.

Incident Response

The loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of the information. Because DCR employees, contractors/vendors, subrecipients, and other third parties may have access to PII and other sensitive data concerning individuals, all have a special responsibility to protect that information from loss and misuse.

Examples of a suspected or actual disclosure of PII include, but are not limited to:

- A laptop or portable storage device containing PII is lost or stolen;
- An email containing PII is inadvertently sent to the wrong person;
- A box of documents with PII is lost or stolen during transport;
- An unauthorized third party overhears agency employees discussing PII about an individual seeking employment or assistance;
- A user with authorized access to PII discloses it for personal gain or to embarrass an individual,
- An IT system housing PII is accessed by a malicious actor; and/or
- PII that should not be widely disseminated is posted inadvertently on a public website.

Individuals with access to PII should not wait for confirmation that a disclosure has occurred before reporting the suspected incident to their supervisor. Such a delay may undermine DCR's ability to investigate the potential disclosure, to protect the PII from continued disclosure, or to mitigate or reduce the risk of harm to potentially affected individuals. In addition, any delay may reduce the likelihood that DCR can recover a lost or stolen device or physical document. Supervisors made aware of a potential incident shall report it to the DCR Deputy Secretary and Internal Audit team.

DCR will comply with the North Carolina Identity Theft Protection Act, N.C.G.S. § 75-60 *et seq*. DCR will report a security breach to: the North Carolina Attorney General's Office; the three major credit reporting agencies (TransUnion, Equifax, and Experian); the N.C. Department of Commerce's General Counsel, Chief Information Officer, and Chief Information Security Officer; and HUD's Privacy Office, Disaster Recovery Mailbox, and grant managers assigned to DCR. If a laptop has been lost or stolen, the incident must also be reported to the State Bureau of Investigation. In the event of a cybersecurity incident involving PII, the event shall be reported in accordance with NCDIT and ESRMO requirements, including submission of the State Cyber Incident Reporting Form within twenty-four (24) hours of confirmation. DCR will also notify the people affected and include the following information:

- General description of the security breach incident;
- Type of personal information breached;
- General description of efforts to avoid further unauthorized access to PII;
- Telephone number where people can call for more information and assistance;
- Advice for people who are affected; and
- Contact information for the major credit reporting agencies, the Federal Trade Commission, and the North Carolina Attorney General's office.

Additionally, if a breach involves PII that DCR received from a federal agency, DCR will follow the reporting requirements in the data sharing agreement with that agency, the applicable Computer Matching Agreement, and/or the applicable System of Record Notice.

Appendix A

Personally Identifiable Information Policy Acknowledgement Form

I have reviewed and acknowledge DCR's Personally Identifiable Information (PII) Policy. I agree to abide by this Policy and take all necessary steps to ensure the privacy and confidential nature of all PII and to protect such information from unauthorized disclosure. I will report any suspected disclosure of PII as described in this Policy.

I further agree that all PII will be stored in a way that is safe from access by unauthorized persons at all times and managed with appropriate information technology (IT) services. Access to PII through program and grant activity will be restricted to only those individuals who need access in their official capacity to perform duties within the scope of work.

_____
Printed Name

_____
Signature

_____
Agency/Organization Name

_____
Date