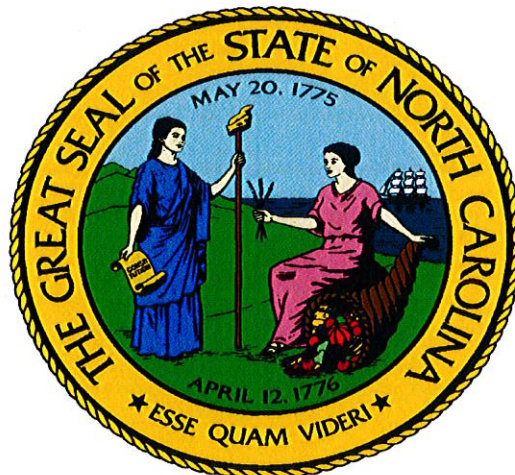


**NORTH CAROLINA DEPARTMENT OF ADMINISTRATION**

# **POLICIES AND PROCEDURES**

---

## **PERSONALLY IDENTIFIABLE INFORMATION POLICY**





## **INTRODUCTION**

This policy applies to the collection, use, security and disclosure of social security numbers (SSNs) and Personal Identifying Information (PII) by Department of Administration (DOA) and the regulation of SSNs and PII.

PII is all "identifying information" as defined by NC Gen. as limited by NC Gen. Stat. §132-1.10 to include:

- Social security or employer taxpayer identification numbers
- Driver's license, state identification card or passport numbers
- Checking account numbers
- Savings account numbers
- Credit card numbers
- Debit card numbers
- Personal Identification (PIN) Code as defined in G.S. 14-113.8(6)
- Electronic identification numbers, electronic mail names or addresses, Internet account numbers or Internet identification names
- Digital signatures
- Any other numbers or information that can be used to access a person's financial resources
- Passwords
- Parent's legal surname prior to marriage

## **POLICY OBJECTIVES**

In order to implement and ensure compliance with legal requirements governing SSNs and PII, DOA Internal Audit will oversee the compliance with respect to the collection, segregation, disclosure and security of SSNs and other PII and the development of related policies. Internal Audit is responsible for reviewing and approving the manner of collection, storage, and transmittal of SSNs and other PII to ensure that adequate controls are in place to protect the sensitive data.

### **016. COLLECTING SOCIAL SECURITY NUMBERS**

Unless specifically authorized by DOA Internal Audit no Division entity or employee shall create a form or electronic template that requires or contains a SSN for any purpose. This prohibition includes the creation of databases, reports, internal spreadsheets or other documents that contain SSNs.

### **017. SEGREGATING/SEPARATING SOCIAL SECURITY NUMBERS**

Pursuant to law, each division entity that properly collects SSNs must segregate/separate SSNs from the rest of the record in some manner that permits SSNs to be easily redacted/removed in the event of a public records request. For example, if a division appropriately collects SSNs in a document or form, the SSN should be on a line by itself so that it can be easily redacted/removed without affecting public information on the document or form. SSNs shall not be included in header or footer information or as part of the document file name.

### **018. DISCLOSING SSNs and PII**

Pursuant to law, divisions may not intentionally communicate or otherwise make available to the general public a person's SSN or PII. SSN and PII are confidential.

Disclosures of SSN or PII to DOA vendors, contractors or other external entities must be reviewed and approved in advance by the DOA Internal Audit. The vendor, contractor or external entity must complete a form (attached)

certifying its compliance with applicable law. The collection of SSNs or PII on behalf of or as requested by another state or federal government entity must be approved in advance by the DOA Internal Audit.

019. **DOA Standard for Collection, Use, Disclosure of SSN and PII**

Proper security measures include but are not limited to locked filing cabinets and offices, password-protected electronic files, and electronic encryption measures. Guidelines for protecting SSNs are as follows:

1. SSNs may not be used as a primary identifier, including as an indexing system for imaged documents. SSNs may be a part of historical databases or imaged documents given its past use as the primary identifier at the Division. The use of such historical databases must be approved by the DOA Internal Audit.
2. Once approval is received from the DOA Internal Audit access to documents containing SSNs must be limited to authorized persons and secured using authorization controls, including passwords.
3. Records, databases, spreadsheets, etc. containing SSNs or PII stored on computers or other electronic devices has be encrypted.
4. All requests for SSNs must be accompanied by a Disclosure Statement stating the purpose of collecting the SSN.
5. DOA or Division employees may not disclose SSNs to unauthorized persons or entities.
6. Transmission of SSNs unencrypted over the internet is prohibited.
7. PII information received from outside
8. Historical records containing SSNs in off-line storage, such as paper, tape, cartridge, fiche, microfilm or magnetic media may be maintained, but access to these off-line records must be limited and secure.
9. All records that are no longer needed must be purged, and disposal of the records must follow State deletion policies and procedures.
10. DOA and Division employees that collect, manage, and disseminate SSNs must undertake annual audits to demonstrate adequate processes and controls are in place that maintain the integrity and confidentiality of the data.
11. Divisions should have disclaimers on the internet pages which enables the public to transmit information when the page is not a secured or encrypted. The DOA employees should provide adequate warning to the public about sending PII and SSN via unsecured email.

020. **SSNS OR PII MAY NOT BE SENT ELECTRONICALLY (BY E-MAIL OR OTHERWISE) UNLESS SUCH DATA IS ENCRYPTED.**

SSNs may not be printed on any materials that are mailed to an individual, unless state or federal law requires that the social security number be on the document to be mailed. The mailing of materials that contain SSNs must be approved in advance by the DOA Internal audit.

Questions regarding these requirements may be e-mailed to DOA Internal Audit Director or Chief Operating Officer (COO).

021. **STATE PRIVACY ACT (SPA) RESTRICTIONS**

Pursuant to the State Privacy Act, DOA shall not deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his/her SSN except refusal to disclose after a request pursuant to the requirements of a statute.

All individuals from whom SSNs are solicited shall be informed of: 1) whether or not the requested disclosure is mandatory or voluntary; 2) by what statutory or other authority the SSN is being solicited; and 3) what uses will be made of the SSN.

022. **NORTH CAROLINA IDENTITY THEFT PROTECTION ACT OF 2005 RESTRICTIONS**

The North Carolina General Assembly enacted the North Carolina Identity Theft Protection Act in 2005 (NCIDTPA). The NCIDTPA imposed restrictions on the collection and segregation of SSNs and upon the disclosure and security of SSNs and PII as follows:

4.1.1 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(1), SSNs shall not be collected from an individual unless authorized by law to do so or unless the collection of the SSN is otherwise imperative for the performance of DOA's duties and responsibilities as prescribed by law. SSNs collected by DOA must be relevant to the purpose for which collected and shall not be collected until and unless the need for SSN has been clearly documented.

4.1.2 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(2), when collecting a SSN from an individual, the SSN must be segregated on a record in an appropriate manner that permits the SSN to be easily redacted in the event of a public records request.

4.1.3 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(3), DOA shall not fail, when collecting a SSN from an individual, to provide, at the time of or prior to the actual collection of the SSN, that individual, upon request, with a statement of the purpose or purposes for which the SSN is being collected and used.

4.1.4 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(4), DOA shall not use a SSN for any purpose other than the purpose stated.

4.1.5 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(5), SSNs and/or PII shall not be intentionally communicated or otherwise made available to the general public. SSNs and PII are confidential except where disclosure is otherwise permitted by law.

4.1.6 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(6), SSNs shall not be intentionally printed or embedded on any card required for an individual to access DOA services.

4.1.7 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(7), unless the connection is secure or the social security number is encrypted, an individual shall not be required to transmit his/her social security number over the Internet.

4.1.8 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(8), an individual shall not be required to use his/her SSN to access an Internet website, unless a password or unique personal identification number or other authentication device is also required to access the Internet website.

4.1.9 Pursuant to N.C. Gen. Stat. § 132-1.10 (b)(9), SSNs shall not be printed on any materials that are mailed to an individual unless state or federal law requires the SSN to be on the document to be mailed. A SSN that is permitted to be mailed may not be printed, in whole or in part, on a postcard or other mailer not requiring an




4.1.10 Pursuant to N.C. Gen. Stat. § 132-1.10 (c)(1), SSN(s) and PII may be disclosed to another governmental entity or its agents, employees, or contractors if the disclosure is necessary for the receiving entity to perform its duties or responsibilities. The receiving governmental entity and its agents, employees, and contractors shall maintain the confidential and exempt status of such numbers.

4.1.12 Pursuant to N.C. Gen. Stat. § 132-1.10 (c)(3), SSNs and PII SSNs and PII may be disclosed for public health purposes pursuant to and in compliance with Chapter 130A of the General Statutes.

023. **FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA) RESTRICTIONS**

024. **HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA) RESTRICTIONS**

Approved by the Secretary of Department of Administration:	 <b>Bill Daughtridge, Jr.</b>
Approval Date:	<b>Version : ADM (V.1) 16-24 - 07/01/2015</b>
Effective Date:	
Revision Date:	

**THIS POLICY SUPERSEDES ALL PREVIOUS  
PERSONALLY IDENTIFIABLE POLICY (PII)**



## DEPARTMENT OF ADMINISTRATION

### STATEMENT OF CONTRACTOR COMPLIANCE WITH

### THE NORTH CAROLINA IDENTITY THEFT PROTECTION ACT OF 2005

\_\_\_\_\_ ("Contractor") hereby certifies that,  
pursuant to section 4(c)(1) of North Carolina General Assembly Session Law 2005-414 (to be codified at section 132-1.8(c)(1) of the North Carolina General Statutes), the text of which is available at <http://www.ncga.state.nc.us/Sessions/2005/Bills/Senate/HTML/S1048v6.html>, Contractor's collection of social security number information from East Carolina University (the "University") is necessary for the performance of Contractor's duties and responsibilities on behalf of the University. Contractor further certifies that it shall maintain the confidential and exempt status of such social security number information, as required by section 4(c)(1).

By: \_\_\_\_\_  
[Signature of Contractor]

Name: \_\_\_\_\_  
[Printed name]

Title: \_\_\_\_\_

Date: \_\_\_\_\_

Division: \_\_\_\_\_

Submitted on behalf of the DOA. by: \_\_\_\_\_  
[Printed name]





## DEPARTMENT OF ADMINISTRATION PII USE REQUEST FORM

Division Name:		Division Director:
Division Contact Phone Number:	Division Contact:	Date of Completion:
Please list the names of all Applications, Databases, Forms or Electronic Templates which Use, Disclose or Store Personal Identifying Information (PII).		
Please indicate the type of PII you are collecting, using, disclosing or storing (e.g. Drivers License Number, Credit Card Number, Account Number, etc.).		
Have you investigated other options to collecting, disclosing or storing PII to meet your business needs? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If yes, please explain the barriers.		
If no, please consider other options prior to submitting this request.		
Please provide the location where data from these forms are stored (PirateDrive, local hard drive, Administrative database, Room #)		
Is data from the form or electronic template distributed or maintained by your division on behalf of an outside vendor or third party? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If yes, please identify the outside vendor and/or third party.		
What is the purpose of collecting the PII?		
Is the requirement to provide the PII voluntary or required for the individual? Provided?		Will service be withheld if not
Do you share any of the PII you collect with others outside of your division? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If yes, please identify: (a) the department and contact person, (b) the purpose for disclosure, (c) method of disclosure (e.g., email, fax, paper copy), (d) type of PII that is shared, other (please specify).		
Do you share any of the PII you collect with outside vendors or third parties? <input type="checkbox"/> Yes <input type="checkbox"/> No		
If yes, please identify: (a) the outside vendors and/or third parties, (b) the purpose for disclosure, (c) method of disclosure (e.g., email, fax, paper copy):		
Is the collection of PII approved by your division director and internal audit? <input type="checkbox"/> Yes <input type="checkbox"/> No - If so, please provide name and contact number for the individual.		
How is access to data and forms or electronic templates that contain PII controlled or restricted (e.g., locked file cabinets, password protection, encryption)? Please describe the process. Attach documentation if needed.		



## **DEPARTMENT OF ADMINISTRATION**

### **DIVISION VETERAN AFFAIRS**

#### **HANDLING OF PERSONALLY IDENTIFIABLE INFORMATION (PII)**

North Carolina Identity Theft Protection Act defines personal information as a person's first name or first initial and last name in combination with identifying information as defined in NCGC14-113.20(b) which includes a social security number, employer taxpayer identification number, driver license number, state identification card, passport number, checking and savings account numbers, credit and debit card numbers, PIN codes, electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names, digital signature's, any other number's or information that can be used to access a person's financial resources, biometric data, finger prints, passwords, and parent's legal surname prior to marriage. Personal information does not include publicly available directories containing information and individual has voluntarily consented to have publically disseminated or listed, including name address, and telephone number and does not include information made lawfully available to the general public from federal, state, or local government records.

It may be difficult and confusing how to implement PII standards but following practices/procedures implemented in VA office can help better understand and comply with State and Federal regulations.

##### **1) IF YOU DO NOT NEED IT – DO NOT STORE IT**

Many offices retain other forms of personally identifiable information (PII) "just because". Review your processes. If you don't need it, don't keep it! Ask yourself, "Are multiple people in your area retaining the same data?" If so, limit the number of staff retaining the data to one person to be responsible for safeguarding the data.

##### **2) PROPER DESTRUCTION OF HARD COPIES**

Once the transaction has been processed, destroy the form. This may require forms/papers with PII information to be cross-cut shredded.

##### **3) INFORMATION TAKEN ON THE PHONE**

Many times it is considered good to take phone calls, emails or some other form of communication to process scholarship application. It is not recommended to act as the customer and input their data for them.

##### **4) CLEAN DESK POLICY**

Forms with PII data should not be left out on desks or in open areas when not needed. Even if leaving the desk for a short period, staff should keep material in a folder and lock the folder in the desk when they leave temporarily. At the end of the day, all PII data should be stored in a secure file cabinet or safe in a locked office with limited access.

- Forms used to collect PII data should be marked "Confidential".
- Forms used to collect PII data should be printed on colored paper to assist with identifying sensitive information that must be safeguarded.

##### **5) ELECTRONIC STORAGE OF PII DATA**

A process should be developed to "mask" the social security numbers in a spreadsheet and spread sheet should also be secured with a password.

**6) NEVER EMAIL PII DATA**

Staff should never use email as a manner of transmitting PII data. Fax machines must be in a secured location. If possible, employees should utilize passcodes to access faxes to ensure control of sensitive information.

**7) DO NOT ALLOW UNAUTHORIZED PERSON'S UNACCOMPANIED ACCESS TO AREAS WHERE DATA IS STORED OR PROCESSED**

This includes other VA staff. As an example, maintenance and janitorial staff should not be permitted in secure areas unaccompanied. This sometimes requires a change in service times.

**8) DOCUMENT DESK PROCEDURES**

To insure continuity when office personnel are out, have all individuals' document daily procedures for their role in the handling of confidential data.