NEW YORK STATE Corrections and Community Supervision **DIRECTIVE**	TITLE **Personal Identifying Information**		NO. 2013 DATE 12/19/2018
SUPERSEDES DIR. #2013; Dated 07/01/2015	DISTRIBUTION A	PAGES PAGE 1 OF 3	DATE LAST REVISED
REFERENCES (Include but are not limited to) Directives #2011, #2012; Federal Trade Commissioner Regulations; General Business Law	APPROVING AUTHORITY		

I. PURPOSE: The purpose of this directive is to control the access to and distribution, storage, and disposition of all forms, reports, and other documentation which contain personal identifying information and to ensure compliance with Federal Trade Commission Regulations (16 CFR 682) implementing the Fair and Accurate Credit Transaction Act of 2003 and with General Business Law, Section 399-h.

II. BACKGROUND: Unauthorized disclosure of personal identifying information may threaten safety and security, is an invasion of personal privacy, is contrary to the public interest, and may violate New York State and Federal law.

III. DEFINITION

A. Personal identifying information shall include any one of the following data elements, unless encrypted within a record that does not also contain the encryption key:

1. Social Security Number;
2. Personal driver's license number or non-driver identification number; and
3. Mother's maiden name, financial services account number or code, savings account number or code, automated teller machine number or code, electronic serial number or personal identification number which may be used alone or in combination with any other information to assume the identity of another person or access financial resources or credit of another person.

B. Inasmuch as inmate possession of personal information on employees increases the risk of employee harassment or other jeopardy, and is likely to deter interested persons from careers in the Department of Corrections and Community Supervision, the Department has determined that the following employee information should be similarly protected from unauthorized disclosure:

1. Employee personal (home) residence address;
2. Employee personal (non-business) e-mail addresses;
3. Employee personal (non-business) telephone numbers; and
4. Employee personal motor vehicle license numbers.

IV. POLICY: Personal identifying information shall be strictly controlled to prevent unauthorized access. All custodians of records which contain personal identifying information shall implement controls to ensure compliance with this directive.

In the event that employee personal identifying information is disseminated to an inmate as a result of a breach in these procedures, the affected employee shall be informed as soon as possible.

Questions concerning access to or use of such documentation should be addressed to the appropriate Deputy Commissioner, the Deputy Commissioner and Counsel, or the Director of Personnel.

V. PROCEDURE

A. Storage: When not in use, forms, reports, and other documentation which contain personal identifying information on Department employees shall be stored in secured spaces or containers (e.g., locked offices, locked file cabinets) or other spaces or containers within a security perimeter which prevents unauthorized access.

B. Access: Access to forms, reports, and other documentation which contain personal identifying information shall be restricted to those who must work with them in their official capacity.

C. Distribution/Dissemination

1. Forms, reports, and other documentation which contain personal identifying information shall be distributed or disseminated only to those who have an official need for such documents or as specified under regulations promulgated by such other agencies (e.g., Civil Service) having original jurisdiction over such documentation.
2. When it is necessary to copy such documentation for persons who are not governed by this directive, such as in response to discovery demands for litigation, the personal identifying information shall be redacted prior to delivery unless other instructions are provided by the Department's Executive staff.
3. When it is necessary to copy such documentation for persons who are not governed by this directive, and the personal identifying information is not to be redacted, a cover sheet shall be affixed to the documentation containing the following statement:

> *The attached documentation contains personal identifying information and is intended only for the official use of the individual or entity to whom it is addressed. Any unauthorized disclosure, dissemination, distribution, or copying of this documentation is strictly prohibited.*
>
> *This documentation must be secured from inmate access.*

D. Disposal of Records Containing Personal Identifying Information: The employee who is throwing away or getting rid of a record containing personal identifying information shall do one of the following:

1. Shred the record prior to disposal;
2. Destroy the personal identifying information contained in the record;
3. Modify the record to make the personal identifying information unreadable; or
4. Take action consistent with commonly accepted industry practices that are reasonably believed to ensure that no unauthorized person will have access to the personal identifying information contained in the record.

E. Breach of Procedures

1. Any staff person having knowledge of a breach of these procedures shall immediately notify his or her supervisor and, as appropriate, initiate corrective action.

   If it is known or appears that an inmate has or may have received or had access to personal identifying information, supervisory staff shall inform the affected employee in writing as soon as practicable, with a copy to the Deputy Superintendent for Administration or Director of Personnel, as appropriate. The Deputy Superintendent for Administration or Director of Personnel shall keep a record of any such breach of procedures and ensure that a copy of the written notice to the employee is placed in the employee's personnel file. The affected employee then has the option to notify his or her bank(s), creditor(s), and the like.

2. A supervisory staff member who recognizes or is informed of a breach of these procedures shall promptly deliver a written summation of his or her findings to the facility Deputy Superintendent for Administration or Director of Personnel, as appropriate. These findings shall include, at minimum, the date, time, and place of the breach, a description of the events or omissions leading to the breach, the name(s) of staff involved, the name(s) and DIN(s) of inmates involved or suspected, and a description of any corrective action taken.