Agency of Natural Resources
Department of Environmental Conservation
Personally Identifiable Information (PII) Policy

Effective Date: May 1, 2019

Signed: Emily Boedecker, DEC Commissioner

VERMONT
Agency of Natural Resources

PURPOSE

It is the policy of the Department of Environmental Conservation (DEC or the Department) to take reasonable steps to protect non-public personal information handled, collected, stored or used in the course of Department functions.

SCOPE

This policy applies to the Commissioner's Office and all Department Divisions and program employees handling, collecting, storing or using records containing Personally Identifiable Information (PII). A record means any written or recorded information, regardless of physical form or characteristics, which is produced or acquired in the course of public agency business.

PII DEFINITION

For purposes of this policy, "personally identifiable information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized persons:

- Social Security number;
- motor vehicle operator's license number or nondriver identification card number;
- financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
- account passwords or personal identification numbers or other access codes for a financial account.

"Personally identifiable information" does not mean publicly available information that is lawfully made available to the general public from federal, State, or local government records

AVOIDANCE OF PERSONALLY IDENTIFYIABLE INFORMATION

The Department shall only collect personally identifiable information when it is required by law or necessary for the implementation of a program.

COLLECTION OF PERSONALLY IDENTIFIABLE INFORMATION

Prohibition. The Department shall not collect any electronic records of personally identifiable information unless it is submitted to you from a state issued O365 e-mail account.

Acceptable means of collecting personally identifiable information. The Department may accept personally identifiable information in a paper format; over a secure ftp server; or through another secure means to transfer information approved by the Commissioner in consultation with the Agency of Digital Services where applicable. The handling of PII, regardless of format, should be restricted to authorized staff.

STORAGE OF PERSONALLY IDENTIFYIABLE INFORMATION

If a program collects paper records containing personally identifying information, that information shall be stored in a locked file cabinet where access is limited to designated staff persons who must have access to this information to perform their job duties. File drawers shall be locked when not in use. The designated staff persons shall securely manage file cabinet keys.

If a program collects electronic records containing personally identifiable information, that information shall be stored in a state-approved networked or cloud storage location (such as the ANR file server or ANR SharePoint Online platform) with access limited to persons who must have access to this information to perform their job duties. The Program Manager shall submit an ADS LANDesk ticket to limit access to designated staff. Microsoft One Drive for Business is not an approved storage location for PII nor are other

cloud storage services such as Google Drive, Drop Box, or iCloud. Please discuss with the Agency of Digital Services your storage requirements if you have questions.

USE OF PERSONALLY IDENTIFIABLE INFORMATION

Personally identifiable information shall always be kept in a secure location when not in use by the designated staff persons. It shall not be left unattended on a computer monitor or desk. All state computers shall be locked while unattended.

Personally identifiable information shall never be physically taken off site by an employee, accessed or stored outside of state-approved file storage locations, or stored locally on non-state issued computers, tablets, or smart phones.

If the State contracts with a person to review personally identifiable information on the state's behalf, contracts shall require that the business conform to the requirements of 9 V.S.A. chapter 62 (protection of personal information) and have systems and procedures in place to ensure that personally identifiable information is protected. The Contract Manager should consult with ADS and the Attorney General's Office through ADS's Procurement Advisory Team in development of said contracts to ensure the most current Information Technology terms and conditions related to data security are included.

When transmitting personally identifiable information internally or to a third party under contract to perform a review function for the Department, the records shall be transferred via e-mail with [SECURE] in the subject line of the e-mail, through the mail, an ADS-approved secure method, or by a secure method supplied by the third party and approved by the Agency of Digital Services. The Agency of Digital Services Email Encryption Guide can be found here: https://vermontgov.sharepoint.com/sites/ADS-IT/HowTo/Encryption%20--%20Microsoft%20Office%20365%20Instructions.pdf

The Agency of Digital Service has enabled Data Loss Prevention rules in Office 365, which includes all Email, OneDrive for Business, and SharePoint Locations. Data Loss Prevention rules will notify the user that files or email may contain personally identifiable information. Employees shall adhered to this policy when handling this information.

DESTRUCTION OF PERSONALLY IDENTIFIABLE INFORMATION

The Department shall destroy records containing personally identifiable information in accordance with the appropriate record retention schedules and procedures.

SECURITY BREACH

If a DEC employee has reason to believe that Department PII information has been breached, the employee must immediately notify their supervisor and division director. The division director shall notify the DEC Commissioner's office and submit an ADS LANDesk ticket to address the breach if applicable to electronic systems.