PERSONALLY IDENTIFIABLE INFORMATION AND SENSITIVE DATA POLICY

TYPE:	POLICY
CATEGORY:	GENERAL
STATUS:	APPROVED
DATE APPROVED:	3/24/2021
DATE REVISED:	3/24/2021
VERSION:	V1.3

City of Albuquerque employees, in the course of their normal job responsibilities, will come into contact with Personally Identifiable Information (PII). It is important for employees to understand their roles in the collection and storage of PII.

1. **Purpose**

   The purpose of this policy is to protect City of Albuquerque's personally identifiable information and sensitive data from unauthorized disclosure and inappropriate use. This policy provides details on how to identify and handle Personally Identifiable Information (PII), the process of securely storing any PII that the organization is required to maintain, and what to do in the event of a disclosure of PII.

2. **Scope**

   All staff, employees, and entities working on behalf of the City of Albuquerque who are using City owned or personally owned devices that connect to the City's network are subject to this policy.

3. **Policy**

   Identifying PII

   There are two (2) types of Personally Identifiable Information (PII) and identification of each type will dictate the actions needed to ensure its safety and integrity. This includes citizens and employees

   - Public PII

     This is information that is available in public sources such as telephone books, employee directories, public websites, etc. the following information can be considered Public PII:
     - First and Last Name
     - Address
     - Work Telephone Number
     - Work Email Address
     - Home Telephone Number
     - General Educational Credentials

- Personal Email Address(es)
- Photos and Videos

- Protected PII
  This is any information which, if lost, compromised, or disclosed without authorization, could cause substantial harm, embarrassment, inconvenience, or unfairness to an individual. It includes one or more of the information outlined below:
  - Social Security Number
  - Username and Password
  - Passport Number
  - Alien Registration Number
  - Credit Card Number
  - Clearances
  - Banking Information
  - Biometrics
  - Date and Place of Birth
  - Mother's Maiden Name
  - Criminal, Medical, and Financial Records
  - Educational Transcripts*
  - Photos and Videos including any of the above
    **Note: Educational transcripts fall under FERPA guidelines, please see the FERPA Compliance Guidelines for details.*

Maintaining PII

During normal job responsibilities, employees may come in contact with either Public of Protected PII, either existing in the City of Albuquerque's network, or as part of a business process. Because Protected PII requires special handling because of potential risk associated with its disclosure, it is important to 1) verify the need for the existence of PII on CABQ systems and 2) ensure that the information is properly secured.

- Verifying the need to collect PII
  Best practice dictates that an organization only collects the least amount of information in order to follow standard business policies. Caution should be taken when collecting Protected PII. The need to collect the information should be periodically reviewed, and if deemed unnecessary, the policy should be altered to reflect the change.
- Collection Policies
  If PII needs to be collected, employees have certain responsibilities in making sure the data is secured. Any written information as a result of a phone conversation must be destroyed via shredding. Physical files that contain PII should be locked in a secure cabinet or room when not being actively viewed or changed. Any PII data collected should not be stored on

the local workstation; it needs to live in a secure location where it can be encrypted and backed up.

- Verifying the need to store PII
  Whenever PII is found living in the City of Albuquerque's network, a determination needs to be made regarding whether the information is needed for an existing business practice, or if it can be securely disposed of. If the information needs to be retained, please contact the Department of Technology and Innovation Security Group for guidance on the best means to secure or dispose of the information properly.
- Authorized Dissemination of PII
  In the event an outside entity would need to have any data that includes Protected PII, said entity would need to confirm that they understand the sensitivity of the information, and the need to properly safeguard it. Once it leaves the City of Albuquerque, the DTI Security Group cannot guarantee its security. Transport of data should be done through secure means (ideally shared through encryption or other secured transport methods.)
- Unauthorized Dissemination of PII
  In the event of an unauthorized disclosure or access of PII:
  - Report the incident to your direct supervisor and to the DTI Security Group
  - Send an email to: ISDHelpdesk@cabq.gov
    - Do NOT forward any compromised information in the email
    - Include the location of the information (email or network location)
    - If email, include the sender and subject (unless the subject contains the PII)
    - Include any other relevant details, such as location and contact phone number
  - Comply with the instructions from the DTI Security Group

DTI PII Oversight

- DTI Security Group will meet monthly to review PII inventory with the Infrastructure Manager
- Infrastructure Manager shall notify DTI Security Group of any changes in PII systems.
- DTI Security Group shall insure the inventory is updated accordingly
- For non-DTI servers DTI Security Group shall review monthly with ISGG and Department Liaisons to ensure PII inventory.

4. Sensitive Data

The following items are examples of sensitive data, but are not limit to;

- 1. Personal identification information such as:
  - Social Security Numbers,
  - Personal identification numbers which may be used other than Social Security Number,
  - Employee home address,
  - Employee home telephone number,

- Information protected by the Health Insurance Portability and Accountability Act of 1996 (HIPAA),
- Information protected by the Family Educational Rights and Privacy Act (FERPA),
- Information protected by the Payment Card Industry Data Security Standard (PCI DSS),
- Information protected by the Federal Information Security Management Act (FISMA),
- Credit card account numbers, expiration dates, and card verification values (CVV)
- Bank account numbers (City, employee, vendor, etc.),
- Computer system IDs and/or passwords.

5. Strategic and Tactical Information

- This includes any data that is considered strategic to the City of Albuquerque and if compromised would provide an exploit to compromise security.
  Examples of strategic data include, but are not limited to;
  1. Telecom and Network diagrams,
  2. Infrastructure layouts,
  3. Server names and IP addresses.
- Neither this policy nor any part of this policy shall be construed to override federal, state, or City statutes and regulations on public information.

6. Enforcement

This policy is for your protection. Violation of this policy could be reported to the appropriate supervisor and could be subject to potential disciplinary action, up to and including termination.

7. Exceptions

Limited exceptions to the policy must be approved by the Director of the Department of Technology and Innovation

8. Definitions

- Personally Identifiable Information (PII): Information which can be used to distinguish or trace an individual's identity, such as his/her name, social security number, biometric records, etc… alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc…
- FERPA: The Family Educational Rights and Privacy Act of 1974 sets forth requirements regarding the rights of students and the obligations of institutions to ensure the privacy and accuracy of education records.

9. REVISION HISTORY

Date	Change	Revision	Signature
03/17/2021	Initial Release	DRAFT	

10. References *(May be modified by TRC)*

- **Payment Card Industry Data Security Standard**
  - **PCI DSS v3.2:** 11.1.2**,** 12.10.1. 12.10.2, 12.10.4, 12.10.6
- **Health Insurance Portability and Accountability Act**
  - **HIPAA:** 164.308(a)(6)(i), 164.308(a)(6)(ii)
- **FBI Criminal Justice Information Services for Law Enforcement/Courts**
  - **CJIS:** 5.3.1, 5.3.2, 5.3.2.1, 5.3.4
- **National Institute of Standards and Technology: Information Technology**
  - **NIST SP800-53 r4:** IR-2, IR-3, IR-4, AR-5, SE-2
- **International Organization for Standardization: Information Technology**
  - **ISO/IEC 27002:2013:** 6.1.3, 7.2.2, 16.1.1, 16.1.2, 16.1.4, 16.1.5, 16.1.6
- **Information Systems Audit and Control Association (ISACA)**
  - Good-Practice Framework: IT Governance and Management of Enterprise IT
  - **COBIT v5.0:** APO01.01, APO01.02, APO01.03, APO01.08, APO07.03, APO07.06, APO13.01, APO13.02, DSS02.01, DSS02.02, DSS02.04, DSS02.05, DSS02.06
- **Family Educational Rights and Privacy Act**
  - **FERPA:** (20 U.S.C. § 1232g; 34 CFR Part 99)
- **Inspection of Public Records Act**
  - **IPRA:** https://www.nmag.gov/ipra.aspx
- **Federal Information Security Management Act**
  - **FISMA:** https://www.cisa.gov/federal-information-security-modernization-act
- **Freedom of Information Act**
  - **FOIA:** https://www.foia.gov/