

CITY OF MARSHALLTOWN, IOWA

POLICY AND PROCEDURES FOR PERSONALLY IDENTIFIABLE INFORMATION AND PROTECTED PERSONALLY IDENTIFIABLE INFORMATION

Original Publication: May 26, 2020

Revised: May 23, 2022
Council Resolution: 2022-141

In compliance with Uniform Grant Guidance in Title 2 Code of Federal Regulation (C.F.R.) Grants and Agreements, Part 200 Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards, it is the policy of the City of Marshalltown, Iowa to protect Personally Identifiable Information (PII) of employees, customers, vendors, contractors, volunteers, etc. The electronic restrictions and safeguards outlined in 2 C.F.R. 200.79 Personally Identifiable Information, and 200.82 Protected Personally Identifiable Information (PPII), along with 2 C.F.R 200.303 Internal Controls, this policy provides guidance for employees, volunteers, agents, etc. with access to PII and PPII.

Personally Identifiable Information (2 C.F.R. 200.79) is any information pertaining to an individual that can be used to distinguish or trace a person's identity. Some information that is considered PII is available in public sources such as telephone books, public websites, etc. This type of information is considered to be Public PII and includes:

1. First and Last name
2. Address
3. Work telephone number
4. Work e-mail address
5. Home telephone number
6. General educational credentials
7. Photos and video

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.

Protected PII (2 C.F.R. 200.82) means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to:

1. Social security number
2. Username and password
3. Passport number
4. Credit card number
5. Clearances
6. Banking information
7. Biometrics
8. Data and place of birth
9. Mother's maiden name
10. Criminal, medical and financial records
11. Educational transcripts
12. Photos and video including any of the above

This does not include PII that is required by law, statute, or regulation to be disclosed, such as a law enforcement or court order right to know.

Internal controls (2 C.F.R. 200.303)

The non-Federal entity must:

(e) Take reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designates as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality.

[78 FR 78608, Dec. 26, 2013, as amended at 79 FR 75883, Dec. 19, 2014]

Procedures

Guidelines on how to maintain and discard PII. All electronic files that contain Protected PII will reside within a protected information system location. All physical files that contain Protected PII will reside within a locked/secured/monitored location when not being actively viewed or modified. Protected PII is not to be downloaded to personally owned employee workstations or mobile devices (such as laptops, personal digital assistants, mobile phones, tablets or removable media). PII will also not be sent through any form of insecure electronic communication e.g. e-mail or instant messaging systems.

Significant security risks emerge when PII is transferred from a secure location to a less secure location or is disposed of improperly. When disposing of PII the physical or electronic file should be shredded or securely deleted.

Incident Reporting

The City Administrator and City Finance Director must be informed of a real or suspected disclosure or breach of Protected PII data within 24 hours after discovery. Examples: misplacing a paper report containing PII, loss of a laptop, mobile device, or removable media containing PII, accidental email of PII, possible virus, or malware infection or a computer containing PII.

Audits

Periodic audits of organization owned equipment and physical locations may be performed to ensure that protected PII is stored in approved information systems or locations. The purpose of the audit is to ensure compliance with this policy and to provide information necessary to continuously improve practices.

Enforcement

Anyone found to be in violation of this policy may be subject to disciplinary action as deemed appropriate based on the facts and circumstances giving rise to the violation.

Records Disposal

Records containing personal data are to be disposed of so as to prevent inadvertent compromise of data and will use a disposal method that will render all personal data unrecognizable and beyond reconstruction. Subject to record retention requirements, documents containing confidential information or restricted release information must be shredded, torn, or cut into pieces such that the information is no longer recognizable prior to it being placed in trash or recycling bins. Likewise electronic storage media (for example, diskettes, compact disks, tapes, disk drives, flash drives, etc.) containing confidential information or restricted release information must be completely erased, reformatted, or destroyed prior to being discarded or placed in trash bins. (The City's IT Contractor will collect, erase and collect a certificate of destruction for each piece of electronic storage media equipment).

Acknowledgement:

I acknowledge that I have received a copy of the Personally Identifiable Information and Protected Personally Identifiable Information. I understand that I am responsible for reading and abiding by this policy. I also understand that the purpose of this policy is to inform me of the City's policy and procedure, and it is not a contract of employment. I understand that the City of Marshalltown has the right to change any provision of this policy at any time through a Council resolution and that I will be bound by such changes.

Signature

Full Name (please print)

Date