Personally Identifiable Information Policy

City of Beaverton Emergency Management (EM) Program

6/3/22

REVISION HISTORY

V1.0	Initial Release	4/13/2022
V1.1	City Cyber Security Policy reference added	6/3/22

I. PURPOSE

This Policy is intended to augment the City's Cybersecurity Policy and describes how the City of Beaverton's Emergency Management Program (EM Program) staff and volunteers are to protect the sensitive Personally Identifiable Information (referred to herein as PII) of our volunteers, manage the authorized use of PII, prevent the intentional or unintentional disclosure or misuse of PII, and respond to the unauthorized use of PII for which the City of Beaverton (City) is responsible in terms of confidentiality and access.

This policy is intended to be used in conjunction with the PII Procedures document to ensure that anyone who collects, stores, manages, accesses, or uses PII, as defined in this policy, on behalf of the EM Program, has clear guidance for access, use and destruction of PII in the course of their assigned roles.

II. SCOPE

This policy applies to all EM program volunteers who have access to or gain access to PII, or potential PII, collected as part of program administration and operations. This includes, but is not limited to:

A. Data maintained electronically

1. The EM Program volunteer database
2. Electronic documents
3. Emails

B. Hard copy – to include but not limited to

1. Printed
    a. Rosters
    b. Reports
    c. Sign-in Sheets
2. Handwritten
    a. Contact information
    b. Phone messages

This document specifically addresses the sensitive PII of the EM Program volunteers but the protection and handling of PII extends to information gathered from the public during Emergency Management staff and volunteer operations including deployments, community events, vaccination PODs and shelter operations. Specific details on the collection, maintenance, use and destruction of PII of members of the public is addressed in the CERT and Beaverton Emergency Radio Team (BERT) Concept of Operations manuals.

III. PERSONALLY IDENTIFIABLE INFORMATION (PII)

A. For this policy, PII is any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

B. Within PII, there is information which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or bias to an individual. This is referred to as "Sensitive PII." There are two types of "Sensitive PII;" "Standalone" and "Paired."

a. Sensitive Standalone PII: PII that on its own is sensitive – Example: Driver's License number

b. Sensitive Paired PII: PII that by itself is not sensitive (e.g., name, physical address, medical conditions) but when paired with another non-sensitive element of PII becomes sensitive – Examples: name and medical conditions or name and physical address.

C. PII that is not considered "Sensitive" is referred to as "Other PII."

D. Any document that contains different levels of PII will be handled in accordance with the procedures for the highest level of PII in it. Example: If a document has a table of volunteer information where five columns are "Other" PII and one column is sensitive, the whole document will be treated as sensitive PII.

E. The definition of PII in this policy is more inclusive than the definition provided in the City's Cybersecurity policy.

> "Personal Information" means information that can be used to distinguish or trace an individual's identity, specifically, an individual's first name or first initial and last name in combination with one or more of the following elements: a Social Security Number (SSN); a driver license number or state identification card issued by the Department of Transportation; a passport number or other identification number issued by the United States; a financial account number, credit card number, or debit card number in combination with any required security code or password that would permit access to a financial account; or any biometric records, such as an image of a fingerprint, retina or iris, that are used to authenticate an individual's identity."

IV. DEFINITIONS

A. **Access** - The physical or electronic ability, right or privilege, to view, modify or use PII. (See Section V.D. of this policy)

B. **Admin User** – A term used for City staff and EM Program volunteers who have been authorized direct access to the volunteer information database through the use of the Admin Tool.

- City Staff refers to ISD and EM Program staff

C. **Breach** – A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, information leakage and data spill.

D. **Other (non-sensitive) PII**: Any PII that is not considered Sensitive (Standalone or Paired) and does not require the same levels of security as Sensitive PII.

E. **Other User:** EM Program volunteers that have need for authorized limited, indirect access to information on an ad hoc basis. e.g. Commander for an activity or exercise.

F. **Personally Identifiable Information (PII)**: Any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual.

G. **Privileged User:** EM Program volunteers who have been authorized limited, indirect access to information in the volunteer database based on their volunteer position.

H. **Sensitive PII**: PII, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. There are two types of sensitive PII, Standalone and Paired.

  a **Sensitive Paired PII:** PII that, by itself, is not sensitive (e.g., name, Id number, Amateur Radio License) but when paired with another sensitive element of PII becomes sensitive– Examples: name and medical conditions or name and physical address.

  b **Sensitive Standalone PII**: PII that on its own is sensitive. Example: Driver's License number.

I. **Third Party -** Third party refers to anyone other than parties authorized to maintain, use and have access to the PII.

  1. EM Program volunteers without authorized access would be considered third parties, as would any individual or entity who is not part of the EM program and is not authorized to gain access to program volunteers' PII.

J. **Volunteer Executive Leadership** – Consists of the top three leadership positions in each Volunteer Group. The top leadership would typically be the Group Supervisor and two Deputy Group Supervisors.

V. REQUIREMENTS

A. **Collection** – The EM Program collects PII and potential PII from volunteers and volunteer applicants (e.g., those who register for the Basic CERT Class) through its online volunteer pages on the City's website for administrative and operational purposes.

  a. Any personal information collected by means other than the volunteer database must be treated as PII per this policy.

  b. See the **PII Procedures** for examples of the PII that is collected and the potential uses.

B. **Storage** –

1. The collected PII data for EM volunteers is on a server maintained by the City's Information Systems Division (ISD). ISD is responsible for ensuring proper cybersecurity safeguards are in place to protect the data.
2. Elements of this PII data, contained in electronic and hardcopy reports and documents, may be stored on other devices and in other locations as needed for its operational and administrative use. This PII will be protected from unauthorized use by the staff or volunteer that is utilizing the information, in accordance with the PII procedures.

C. **Management –** The PII is managed by EM program staff and designated EM volunteer staff.

1. Volunteer Staff in positions that involve management of program volunteer data, including providing reports to staff and other volunteer leaders, are provided direct access.
2. Provision of access is based on reviewing and acknowledging, by signature, the City's cybersecurity policy, this PII policy and its procedures.
3. See the **PII Procedures** document for details on the management process.

D. **Access -** Access to volunteer information will be based on assigned roles, responsibilities, and tasks. There are two levels of access: Direct and Indirect.

1. Direct Access is access to view and modify the information maintained in the database.

    a. All volunteers will have direct access to their own personal information to maintain that information.

        i. A website log-in and password are required for them to access their data.

b. Direct access to information stored in the database for administrative and operational purposes is limited to EM Staff, ISD programmers, and volunteers designated as Admin Users (See Section IV.C. Management).

i. Direct access as an Admin User requires:

 A valid log-in for the City's network.

 Access authorization is set within the database's security settings by ISD.

c. Before having direct access, volunteers will:

i. Hold a position that requires Direct Access to the data.

ii. Successfully complete a background check.

iii. Review and acknowledge, by signature, the City’s cybersecurity policy, this PII policy and its procedures.

iv. Complete an orientation/training on using the database

v. Complete the cybersecurity training required by the City’s Cybersecurity Policy.

2. Indirect Access is access to information generated from the database in the form of reports.

a. Indirect Access to information generated from the database will be provided in reports based on administrative and operational needs. (See the **PII Procedures** for the types of reports, the information in them, and the positions/roles that may need them.)

b. Before having indirect access, volunteers will

i. Be in a leadership position that requires some elements of personal information to accomplish the roles and assignments of that position. (Example: Cooling Shelter Coordinator)

ii. Successfully complete a background check.

iii. Review and acknowledge, by signature,

the PII policy, and procedures.

E. **Compliance – anyone with access to or use of** the collected information must:

1. Access, collect, store, manage, or use only for official Beaverton Emergency Management program business;
2. Comply with this PII policy and the associated PII Procedures;
3. Comply with data security policies, standards, and laws, described in Section VIII of this policy, which the City is required to follow;
4. Securely store and protect PII from misuse from third parties as outlined in the PII Procedures;
5. Not share passwords or log-ins uniquely provided to them that would permit an unauthorized individual to access PII; and
6. Promptly report any known or suspected violations of this PII Policy to the Group Supervisor or EM Program Staff in accordance with the PII Procedures.
7. Delete or destroy electronic and hard copy documents and reports containing PII in accordance with the PII procedures.

VI. Disposal/Destruction of PII

A. Hard copy and electronic copies of documents, notes, spreadsheets containing PII that are no longer needed will be disposed of following the process detailed in the **"Procedures for PII"** document.

VII. Response to Breach of PII

A. Any actual or possible unauthorized access to PII shall trigger the response detailed in the **"Procedures for PII"** document**.**

VIII. Background and References

The following standards, policies, and laws directly influence this PII Policy:

A. City of Beaverton Cybersecurity Policy

B. Payment Card Industry Data Security Standard (PCI-DSS);

C. Oregon Consumer Identity Theft Protection Act, ORS 646A.600 to 646A.628;

D. Federal Bureau of Investigations Criminal Justice Information Systems (CJIS) Policy;

E. Gramm-Leach-Bliley Act (GLBA); and

F. Health Insurance Portability and Accountability Act (HIPAA).

If two or more of the above have similar requirements that the City must follow, the Emergency Management Program will follow the more restrictive standard, policy, or law.