PROCEDURE: MAINTAINING PERSONALLY IDENTIFIABLE INFORMATION (PII) WITHIN THE CITY'S EMERGENCY MANAGEMENT PROGRAM

REFERENCE: Emergency Management Program PII Policy

REVISION HISTORY

V1.0	Initial Release	4/13/2022
V1.1	Added breach response by city staff	6/3/22

Purpose:

This procedure is to be used by Emergency Management (EM) Program staff and volunteers to:

- Protect the sensitive Personally Identifiable Information (PII) of our volunteers, (referred to herein as PII),
- Manage the authorized use of PII,
- Destroy documents containing PII that are no longer needed
- Prevent the intentional or unintentional disclosure, or misuse of PII, and
- Respond to the unauthorized use of PII.

Background:

The Emergency Management Program collects PII and potentially PII information 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. Some of the information gathered and maintained is sensitive PII which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or bias to an individual.

Definitions:

See the **"Emergency Management Program PII Policy"** document for definitions

Procedures Sections:

SECTION 1. Compliance

A. PII will be collected, stored, accessed, and used for official Beaverton Emergency Management program business only and will be done in accordance with the EM Program's **Personally Identifiable Information Policy** and these procedures.
B. Any known or suspected violations of this PII Policy, whether or not it results in the PII being viewed or used by an unauthorized person, will be reported to the appropriate Group Supervisor or Emergency Management Staff in accordance with Section 7.

SECTION 2. Collection of PII

A. The Emergency Management Program collects PII and potentially PII information from volunteers and volunteer applicants (for administrative and operational purposes. (See the ATTACHMENT A for examples of the PII that is collected and the potential uses).

B. The collection of PII is primarily through the EM Program's online volunteer section of the City's website. It could also be collected through other means, including sign-up lists during community events.

C. Typically, EM Staff and volunteers only collect the elements of PII that are outlined in these procedures and are within the scope of their position.

D. Additional elements of PII, identified by EM Staff as necessary for administrative or operational purposes, may be collected by staff or designated volunteers. Those volunteers will need to have a signed PII Acknowledgement Form (see ATTACHMENT B).

E. All PII, regardless of how it is collected, will be provided the appropriate levels of protection discussed in these procedures.

SECTION 3. Storage of PII:

A. The primary storage location of PII data is on a City of Beaverton server maintained by the City's Information Systems Division (ISD).

B. As required for EM Program administrative and operational purposes, elements of volunteer PII may also be maintained by EM Staff and authorized volunteers on:

   1) City devices, including laptops and Cell phones. ISD is responsible for ensuring the proper cyber security safeguards are in place to protect the data. Additionally, access to these devices is protected by passwords or similar access control (biometrics/fingerprint).

   2) Personal devices, including laptops and cell phones. The individual maintaining the data on the device is responsible for ensuring the proper cyber security safeguards are in place to protect the data and will acknowledge that requirement when they sign the PII Acknowledgement Form. Additionally, access to these devices must be protected by passwords or similar access control (biometrics/fingerprint).

   3) A cloud storage location approved by both EM Staff and ISD (i.e., Office 365 OneDrive). Use of such locations must meet ISD requirements for maintaining city information and data. Access to the storage location must be protected by passwords or similar access controls.

C. As required for EM Program administrative and operational purposes, elements of volunteer PII may also be maintained by EM Staff and authorized volunteers in hard copy formats including, but not limited to, reports, forms, and notes. The individual maintaining the data in its hard copy format is responsible for ensuring that its properly safeguarded and destroyed when no longer needed so that the information cannot be accessed by unauthorized individuals. The need to protect PII in hard copy formats will be acknowledged by signing the PII Acknowledgement Form.

SECTION 4. Access to PII:

A. There are two levels of access: Direct and Indirect.

B. Direct Access

1) All volunteers will have direct access to their personal information to maintain that information. Access is by login to the Volunteer Web site maintained by ISD.

2) Direct access to the information stored in the database is limited to EM Staff, ISD programmers, and volunteers designated as "Admin Users."

3) Access is requested by completing Attachment B, "Acknowledgement of PII Policy and Procedures"

4) See the PII policy for details on requirements for access and other Direct Access Information.

5) See ATTACHMENT B - PII Acknowledgement Form

C. Indirect Access

1) Indirect Access is information generated from the database in the form of reports; printed and electronic. See ATTACHMENT C for the types of reports and the information in them.

2) Access is requested by completing Attachment B, "Acknowledgement of PII Policy and Procedures"

3) See the **PII policy** for details on requirements for indirect access.

4) Indirect access is typically limited to:

   a. EM Staff.

   b. Executive Leadership of each Volunteer Group.

   c. Member Services Unit positions.

   d. Volunteers assigned to help enter/update event and training information in the system.

   e. Team Leads

   f. Project Leads (i.e., MayDay Exercise Planning Lead)

g. Incident Commanders (IC) for Exercises, Incidents and Events.

h. Project Specialists

SECTION 5. <u>Management of PII:</u>

A. The PII is managed EM program staff and designated volunteer staff.

B. Selecting volunteers for positions requiring access:

1) Volunteer Groups' leadership will identify volunteers for possible assignments to positions or roles/responsibilities that require access.

2) Supervising leadership position will interview the volunteer(s) whose position/role requires access to determine suitability, including their awareness of the importance of maintaining and protecting PII.

3) If the supervising leadership position determines the volunteer is a good fit for the position, they will have the volunteer read the PII Policy and Procedures and have them sign a PII Acknowledgment Form (See ATTACHMENT B)

4) The signed PII Acknowledgment Form (See ATTACHMENT B) will be returned to the appropriate Group Supervisor for validation and signature. Once signed, the form will be sent to EM Staff.

C. Volunteer Executive Leadership will be responsible for:

1) Maintaining the list of positions and volunteers within their groups who are authorized direct and indirect access.

2) Ensuring the proper process is followed for approving direct and indirect access.

3) Ensuring the PII acknowledgment form has been signed and maintaining the form until the volunteer is no longer in a role or assignment requiring access.

4) Removing volunteers from the list when they no longer have a role or assignment that requires access.

5) Notifying EM staff within 24 hours when volunteers leave positions and no longer need direct access to the database.

6) For Privileged and Other Users – Update Indirect access authorization within the database's profile settings.

7) Train the volunteers to accurately and appropriately maintain the database.

D. EM Program Staff will be responsible for:

1) When a signed PII Acknowledgement Form is received, EM Staff will confirm:

a. That the form is completed correctly and signed.

b. The assignment of the volunteer is to a role/position requiring direct and/or indirect access.

c. That a background check has been completed on the volunteer.

d. For Admin Users

i Ensure that the volunteer completes the required cybersecurity training.

ii Submit a Work Order to ISD requesting that the person's log-in be established as an "admin user."

e. If the position is validated, EM staff will sign off on the form and return the completed/approved form to the appropriate volunteer group leader.

2) When notified that a volunteer with “Admin Privileges” has left their position, EM Staff will submit a Work Order to ISD, within 24 hours, to have those logins removed from the authorized user’s list.

E. All reports, plans and documents created with PII will be maintained in accordance with city and state retention requirements.

   1) One file copy will be maintained on the city network or in the appropriate file cabinet in the EM Office.

   2) The Emergency Management Program Specialist will coordinate the destruction of all electronic and hard copies of plans, reports and documents.

F. Report generation and distribution will be by direct access (Admin) users to indirect access users. This will occur in one of two ways:
   1) Push model – reports that are part of an administrative process, generated and distributed without a formal request. Examples: Geo team contact list after a class graduation, roster and sign-in sheet for a planned event.
   2) Pull model – indirect users request a report appropriate to their assignment that an admin user approves and generates.
   3) Reports may be, as appropriate, distributed electronically or hard copy, or both.

SECTION 6. <u>Disposal/Destruction of PII</u>

A. All hard copies of documents and notes containing PII will be destroyed by shredding:

   1) The shredder in the EM office is available for use.

   2) Large documents or a large number of documents can be given to EM Staff, who can place them in a secured shred bin at the Public Safety Building.

   3) Personal shredders can be used as long as they are "crosscut" shredders. Shredders that cut pages into long strips are not adequate.

B. Volunteers in the database who have been "Inactive" for more than 4 years will be deleted from the database.

C. Electronic copies of documents containing PII maintained on the City's network or cloud storage must be deleted when no longer needed for their specifically authorized use.

   1) Any associated electronic "Trash Cans" must be emptied after the documents are deleted

   2) PII documents will not be maintained beyond their intended use, even if it makes things "convenient." The longer it is maintained, the greater the risk of inadvertent access or loss of control.

D. Electronic copies maintained on city or personal devices must be deleted immediately when no longer needed.

   1) Any associated electronic "Trash Cans" should be emptied after the documents are deleted

   2) Copies must be deleted from any physical or virtual (cloud) backup drives.

SECTION 7. <u>Response to Unauthorized Access to or Loss of Control of PII</u>

A. Anyone who becomes aware of an actual or possible unauthorized access to or use of PII must report it immediately to their Volunteer Group Supervisor or EM Staff.

   1) If the first person in the chain of command that you would make the report to may have been responsible, the person must make the report to the next person in the chain of command above them.

   2) The report should include:

      a. The nature of the PII (Database or a report) and what it contained.

      b. The circumstance surrounding how the unauthorized access was obtained and or how the information was used.

B. When Volunteer Group Supervisors receive information about an actual or potential unauthorized access to or use of PII they will notify a member of the EM Staff immediately and if possible, take actions to secure the PII.

C. EM Staff, when notified, will:

1) For Unauthorized Access to information stored in the database or on the city's network:

   a. Notify ISD.

   b. Take the steps necessary to secure the PII with ISD assistance.

   c. As applicable, inform the City Attorney and coordinate with the City Attorney's Office regarding notification of volunteers whose information may have been disclosed or accessed.

   d. Begin investigating with ISD assistance how the unauthorized access and/or use occurred.

2) For Unauthorized Access to reports, plans and documents created with PII and not on the city network (e.g., hardcopies):

   a. Take the steps necessary to secure the PII.

   b. As applicable, inform the City Attorney and coordinate with the City Attorney's Office regarding notification of volunteers whose information may have been disclosed or accessed.

   c. Begin investigating how the unauthorized access and/or use occurred.

3) Notify BPD if the actions appear to be a criminal act. This would include but is not limited to:

   a. Forced access to physical data.

   b. Hacking or other similar illegal access to electronic data.

   c. Use of the data in a criminal manner like identity theft

D. Disciplinary procedures, as outlined in the Volunteer Disciplinary Policy, will be warranted if:

1) The unauthorized access to or use of PII was deliberate/intentional by a volunteer.

2) The unauthorized access to or use of PII resulted from gross negligence by a volunteer in handling/maintaining the PII or due to a violation of the PII Policy and these procedures.

E. A review of PII Policy and Procedures will be conducted to determine if there is a gap that needs to be addressed.

F. Additional information/training may be required depending on the nature of the unauthorized access/use of the PII.

SECTION 8. Protection and Use of PII

(Note: This section will be built out as part of the implementation phase of the PII Project)

A. This section provides best practices for the use of PII, which will be followed to help ensure the protection of the volunteer PII maintained by the Emergency Management Program.

1) When sending an email with multiple recipients, place your email address in the "To:" line and put all the recipients in the Blind CC (BCC) line.

2) Do not leave PII out where it can be seen by others. This includes leaving a computer log-in and screen on, as well as leaving hard copies of PII laying out in the open.

3) Do not store PII in a shared folder or on a shared device that can be accessed by others who do not have need or authorization to see the PII.

4) Only provide the level of access to PII that is authorized by the Policy AND is needed for the task/activity.

B. Unit and Committee lists
    1) Authorized indirect users will routinely use PII to contact their 'team".
        i. This information is closely held and not provided to third parties on the team.
        ii. Both standing and ad-hoc committees often have a need to share information with each other and passing ALL communication through the unit leader is impractical.
    2) A unit may establish a communication list to be used among the team for the time they are functioning as a group.
    3) This list is maintained by the unit leader and is kept separate from any information provided by the City.
    4) Before this information is solicited, the unit leader will communicate the following to all unit members, either verbally or electronically:
        a. This information is provided by the unit members to facilitate communication within the team and will be used for no other purpose
        b. A member may refuse to provide some or all PII information with "third party" members of the Unit or committee without impacting their status in the unit or as an Emergency Management volunteer
        c. When the work of the unit is complete, the information will be destroyed.

C. Voluntary Release of PII - An individual volunteer is allowed to provide or exchange PII with other volunteers but this information is not protected by Emergency Management Policy or procedures.

Attachment A – Types of PII

This table is a list of the PII specifically maintained in the Volunteer Data Base and includes the intended use of the information and the category of PII for each. This list may not be all-inclusive as additional information may be provided by volunteers in the comments section of their registration form.

Element of PII	Original Intended Use	Stand alone	Paired	Other PII	Not PII
CERT ID #	Unique Identifier. Displayed on IDs, on passport tags on vests, and sign-in sheets			X	
Customer Status • Active • Reserve • Inactive	Means of identifying levels of engagement of CERT members which also indicates if they want to still receive information and updates. (Inactive means they do not want to be contacted)				X
Name (First and Last)	Means of identifying CERT members and required for Background check			X	
Date of Birth	Required for Background Check and to determine if they meet the minimum age requirement for attending the training		X		
Age	suitability of assignment				X
Email Address	Primary means of contact/communications from the EM Program and the CERT Organization			X	
Physical Address	- Required to determine eligibility to participate in Beaverton CERT (must live or work within Beaverton School District Boundaries). - Used to designate Geo Team - Used generally to show clusters of CERTs for the purpose of establishing rally points		X		

Mailing Address (if different from physical address)	- Used to send things to CERTs when they can't pick them up (certificates, id cards, passport tags, lost items) - Also used during audits of Customer Status when no responses are received by email and phone.		X		
Emergency Contact Information • Phone • Name • Relationship	Needed in case the CERT member experiences a medical emergency during exercises, trainings, events, or incidents/deployments.		X		
Home Phone	- Used during audits of Customer Status when no responses are received by email. - May be used by EM staff for "welfare/wellbeing" follow up after a medical emergency or traumatic experience.		X		
Cell Phone	- Primary means for emergency notifications and call-outs particularly for CERTs on specialty teams. - Alternate means of contact for "welfare/wellbeing" follow ups and for confirming participation in upcoming events		X		
Cell Provider	- Required by the mass notification systems used to send emergency notifications and call-outs to CERT members				x

Employer	- Required to determine eligibility to participate in Beaverton CERT (must live or work within Beaverton School District Boundaries). - Used to designate Geo Team - Used generally to show clusters of CERTs for the purpose of establishing rally points		X		
Work Phone and Ext	Unknown *Not needed- To be deleted in Phase 3*				
Ham Call Sign	Means of identifying CERTs who are licensed HAMs It should be noted that this information is publicly available on the FCC web			X	
Background Check Date	Used to determine when the last background check was run on the CERT member. Depending on their engagement – like Reunification Team – they go through the background check more frequently than someone who is not on that team.				X
Driver's License Information • # • State • Gender • Expiration Date	Required for background check to ensure that there is no criminal history that could be of concern with their involvement in CERT Note: Since this information is only used together it is considered Standalone.	X			
Any Physical Limitations	Used to determine if any special considerations are required for their participation in events, incidents, trainings, and exercises per ADA requirements		X		

Skills	List of skills that the CERT member has (self-reporting) - Could be used for selective call-outs of people reporting to have certain skill sets. - Future use could include designations on vests or ID cards indicated confirmed skills or certifications (i.e., Wilderness First Aid, Traffic and Crowd Management)				X
CERT Team Area	Geo Team area CERT member is assigned to				X
NAC Neighborhood	Which NAC Neighborhood a CERT member lives in			X	
Class Completions	Which Basic CERT Class the member completed				X
Event, Training, Activities, Incident Participation	Tracks the events, trainings, incidents, and activities the CERT has participated in. Used in general for grant and budget reporting purposes and specifically for recognizing levels of involvement/participation (i.e., work 4 events and you get a CERT ball cap)				X
Specialty Teams - Medical Team - Parent Reunification - TBD	- Tracks who is on what specific specialty teams. - Used for identifying who should be contacted for specific trainings, exercises and drills - who needs a more frequent background check? - Setting up specific team lists for call outs.				X

Photo	- Picture for use on official CERT ID - In extreme cases has been used to advise BPD and TVF&R of "rouge" CERT members who have been operating outside of their authority at incident scenes and were no longer members of the Beaverton CERT program		X		

Attachment B - ACKNOWLEDGEMENT OF PII POLICY AND PROCEDURES

Name of Volunteer: _____ (Print or type)

Position or Role requiring PII Access: _____

Type of Access:

☐ Direct Access - Access to the information maintained in the database.

☐ Indirect Access - Access to information generated from the database in documents including, but not limited to rosters, sign-in sheets and reports.

☐ Both

Volunteers with the City of Beaverton's Emergency Management Program may have access to what this agreement refers to as "personally identifiable information (PII)."

Depending on assigned position or role, volunteers may have access to PII in electronic or hardcopy formats. Both formats will be handled and protected to the same level.

By signing this agreement, I acknowledge that I:

- Have read and understand the PII Policy.
- Have read and understand the PII Procedures.
- Understand the level and types of PII I am authorized to access within my assigned roles and responsibilities.
- Agree that if I have a legitimate need to maintain the information electronically on a personal device, including cellphone, tablets, computers, or laptop, that:
    - The device will be protected with a password or other forms of authentication like biometric scan.
    - The security protection software on the device will be up to date and turned on.
- Agree to only access and use the volunteer information maintained by the Emergency Management Program for official Emergency Management purposes only.

- Agree to abide by the established PII Policy and Procedures.
- Know that if I breach my responsibility regarding the protection and use of PII that I may be subject to disciplinary action as outlined in the Disciplinary Policy and Procedure.

Signed: _____ Date:_____

Approvals:	
Group Supervisor:	(printed)
The listed volunteer has been vetted and is appropriate for filling the listed position and the level of access indicated is correct.	
Signature:	
EM Staff:	(printed)
The listed volunteer is Authorized access to PII within the scope of their assigned position or role.	
Signature:	

Volunteers needing Direct Access, will need to complete ISD's required cybersecurity training.

 Completion of Cybersecurity Training verified:

Date Training Completed: _____

Verified by (EM Staff): _____

Date verified: _____

ATTACHMENT C – The PII Contained in Standard Reports

This is only a sample list of the reports that contain elements of personal information. Because of the continuing growth of the volunteer programs additional reports or documents may be developed.

1. Background Check – sent electronically to Beaverton Police Department
    a. First name,
    b. Last name,
    c. Middle Name,
    d. Gender
    e. Date of Birth
    f. Driver's License Number
    g. State
    h. Expiration Date

2. GeoTeam contact lists sent to GeoTeam leads (Digital)
    a. First name,
    b. Last name,
    c. email,
    d. home phone number
    e. Text phone number
    f. CERT ID # and or Amateur Radio Call Sign

3. Sign-In Sheets (Print) [Does not contain sensitive PII]
    a. First Name,
    b. Last Name,
    c. CERT ID # and or Amateur Radio Call Sign

4. Event Rosters (Print)-
    a. First Name,
    b. Last Name,
    c. *CERT ID #,*
    d. email,
    e. Emergency Info (event or exercise dependent)
    f. Phone Numbers (event or exercise dependent)