Personally Identifiable Information (PII)

Definition

Personal Identifiable Information (PII) is defined as:

> Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

https://www.dol.gov/general/ppii

Protohaven and PII

As a membership- and volunteer-based organization, protohaven collects and stores various PII relating to its members and volunteers.

This includes:

- Full name information (as reported by members)
- Contact information (physical address, email, phone number, discord ID etc.)
- Demographic information voluntarily reported by members (socioeconomic, gender, race, neurodiversity and others)
- Donation, class attendance, tool clearance, membership, storage, volunteering and other records

- Banking, credit card, and other payment/transaction information (stored in third party, PCI DSS compliant systems)

PII is present in the following systems that we use:

- Neon CRM / Neon Pay
- Airtable (esp. Instructor Capabilities, Volunteer, and Sign Ins tables)
- Cronicle (in logs of completed jobs)
- Bookstack (user accounts use full name)
- Discord (member accounts use full name)
- MQTT (status updates include member clearance info)
- Sheets (in instructor logs, user sign-ins)
- Square (full names, contact info, payment info)

Consider this list a baseline - **if you see PII present in other systems, please add it to this list.**

Confidentiality Agreement

The following agreement must be signed and submitted to Protohaven staff or the board before PII-involving work is attempted:

Volunteer Confidentiality and Intellectual Property Agreement.pdf

PII Policy for Software Devs

This policy applies to all volunteers, software developers, and maintainers who interact with systems containing member data at Protohaven.

Access Controls:

- Only authorized volunteers with a defined need-to-know basis will have access to PII.
- Where possible, per-user access is granted through unique user credentials.
- Credentials used by automation must be access restricted, and must only be stored in Bitwarden or on Protohaven servers. **DO NOT store credentials used by automation on developer laptops or PCs.**

Data Minimization:

- Software should only collect and process PII that is strictly necessary for its function.
- Do not store sensitive data locally; instead use secure, centralized systems like Neon CRM and Airtable.

Encryption:

- All PII must be transmitted using encrypted protocols (e.g., HTTPS).
- Any PII stored must be encrypted both at rest and in transit. Third party storage (Neon CRM, Airtable) does this encryption automatically for us.

Data Retention and Deletion:

- PII should be retained only as long as required for its intended purpose.
- Upon member request, PII must be securely deleted from all relevant systems.

Volunteer Responsibilities:

- Volunteers handling PII must undergo basic training on data protection principles. That includes reviewing and understanding the contents of this page, and especially signing the confidentiality agreement above.
- Any suspected or actual data breaches must be reported immediately to Protohaven leadership.

Third-Party Integrations:

- Software interacting with third-party services must ensure compliance with this policy and verify the third party's data protection measures.
- Avoid exporting PII unnecessarily to external systems without explicit authorization from Protohaven leadership.

Audit and Monitoring:

- Regular audits will be conducted to ensure compliance with PII policies and identify vulnerabilities.
- Logs of data access and modifications must be reviewed periodically.

Incident Response:

- In case of a data breach, affected members must be notified and mitigations enacted.
- Root cause analysis and an action plan must follow the initial response, to prevent recurrence of the same data breach.

Policy Updates and Communication:

- This policy will be reviewed annually or whenever significant changes are made to the systems.
- Updates will be communicated to all affected volunteers and members promptly, ideally before changes are made.

Member Rights:

- Members have the right to request access to their data, updates to incorrect information, or deletion of their PII.

- Requests should be processed within 30 days if possible, with updates and confirmation provided to the member.

Revision #6
Created 17 January 2025 15:08:02 by Scott Martin
Updated 17 January 2025 21:31:05 by Scott Martin