Oregon IDA Security Documentation for Handling Donor Information

Neighborhood Partnerships understands that the confidentiality and integrity of Oregon IDA Tax Credit contributors' information are vital. In 2016, the Oregon Department of Revenue requested that we collect Social Security Numbers or Employment Identification Numbers from IDA Tax Credit donors. This will help the Department of Revenue connect contributions to tax returns. Neighborhood Partnerships (NP) uses a multi-layer approach to keeping contributor personal information secure. Donor information will never be shared with anyone besides the Oregon Department of Revenue.

Confidentiality and identity theft

NP has a responsibility to protect the privacy of all NP employees, Board members, program participants, volunteers, contributors and business partners. NP employees shall refrain from unauthorized disclosure of nonpublic or personal information regarding NP's program participants, Board, staff, investments, business intentions, purchasing and contracting activities.

Further, NP and its employees have the responsibility to protect privacy and prevent identity theft by protecting the personal information of program participants, employees, donors, volunteers and vendors who are required to provide personal information. "Personal information" means an individual's first name or first initial and last name in combination with a Social Security number, driver's license number, passport or U.S. ID number, financial account number, or credit or debit card number, as well as personal contact information such as address, email and phone number.

Protection of this information is achieved through a control environment, risk management and monitoring. Information is "double locked": keeping hard copy records in a locked file cabinet or locked room within a locked building, or electronic records in a permission or password protected folder within a password protected server.

NP's management determines which employees may have access to personal identifiable information. Access granted is documented, reviewed periodically and revoked immediately upon exit/termination.

NP performs criminal background investigations when hiring all new employees. Employment is contingent upon successful completion of the background investigation. New employees are required to review and sign the following:

- Confidentiality Agreement
- Employee Handbook which includes sections on Information Technology Security and confidentiality of data

NP requires a criminal background check for contractors and vendors who in the course of performing their service may have access to protected information.

Storage of Donor Information

NP stores digital information in a secure Salesforce.com database. Salesforce.com service is collocated in dedicated spaces at top-tier data centers. You can read in detail about their security protocols by requesting from NP a copy of Salesforce's SOC Reports. NP follows Salesforce.com customer security recommendations including SMS identity confirmation for any log in attempts from an unknown source. The users who have access to SSN and EIN information in Salesforce are limited by a certain profile setting. Authorized personnel are prohibited from accessing the Salesforce.com database outside of NP's office. When staff with Salesforce.com access authority leaves employment with NP, their access is de-provisioned immediately.

Salesforce.com database fields that contain SSN and EIN information are encrypted with 128-bit master keys and use the Advanced Encryption Standard (AES) algorithm.

Additionally NP uses secure internal servers, located onsite in a locked storage area.

Passwords

NP maintains a "strong password" policy as outlined in the Employee Handbook, and follows industry best practice for maintaining password secured hardware. All passwords are confidential and unique.

Receipt of Personal Information

NP accepts documentation with personal information such as Social Security Numbers or Employment Identification Numbers in the following three ways:

Mail

NP has a redundant mail opening policy. This policy and NP's money handling processes are audited on a yearly basis by an external audit firm.

Per direction from the auditors, we have appointed specific staff members to open the mail. NP requires two mail openers to open mail and log checks. Checks are stored in the safe and donor paper records in a locked cabinet.

Fax

NP maintains a fax machine secured in a locked room accessible by all staff members. The machine is checked daily to retrieve incoming faxes. Donor forms are stored the forms in a locked cabinet or safe.

Online

Currently, NP does not collect personal information through online means. At this time, all personal information must be submitted by mail, fax or over the phone.

In Sept. 2014, NP underwent a security audit to harden our online properties from attack. NP follows all best practices regarding website administration and utilizes HTTPS (SSL/TLS) so pages cannot be intercepted or modified in transit.

NP collects donation payment via Authorize.net. Authorize.net utilizes industry-leading technologies and protocols, such as 128-bit Secure Sockets Layer (SSL) and they are compliant with a number of government and industry security initiatives. You can learn more about their security protocols by requesting from NP a copy of Authorize.net's SSAE-16 report.

Phone

Donors may call in with their personal identifiable information. That information will only be accepted/collected by staff designated by management. The information will be recorded directly into Salesforce.

Important: NP does not accept credit card payment of donations over the phone.

In 2016, NP will be implementing a secure portal for submitting donor information online. More information on this process will be available shortly.

Preparing acknowledgement letters

All hard copies of donor forms are transferred hand to hand or stored in the safe or locked cabinet. Acknowledgment letters do not contain contributor SSNs or EINs.

Email Deletion Policy

NP strongly discourages the transfer of personal information via email or emailed documents.

NP does not retain email which contains either in the body, or as an attachment, an individual's social security number. However, the email will be printed, as will any attachment be printed before the email is deleted. Any printed email and attachments with SSN or EIN are stored under lock and key as described above.

Transfer of Personal Information

Once-yearly NP transfers contributors' personal identifiable information to the Oregon Department of Revenue via secure portal. Access to this portal was granted by the Oregon Department of Revenue to one NP employee designated by NP management.