Chapter:	Finance and Fund Development		
Title:	Donor Information Privacy and Security		
Policy: ☒ **Procedure:** ☐	**Review Cycle:** Triennial **Author:** CDO/FDC	**Adopted Date:** 02.2024 **Review Date:** 02.2024	**Related Policies:** Standards of Conduct Information Management and Security

Purpose:

Hopeful Horizons (HH) has established its Donor Information Privacy policy to clarify our commitment to and expectations for the protection and proper use of donor personal and payment information and to demonstrate practices consistent with industry standards and best practices.

Scope:

This policy applies to:

☐ All HH Staff ☒ Selected HH Staff, as specified: Fund Development Staff, CEO

☒ HH Board Members ☒ HH Volunteers

☒ Other: Donors

Policy:

HH is committed to respecting the privacy and security of its financial and in-kind donor information, whether the donation is made online, by mail or another method. HH and its third party providers use industry standards to safeguard and protect donor information consistent with the Donor Bill of Rights.

A. Roles and Responsibilities: The Chief Development Officer (CDO) and Fund Development Coordinator (FDC) are responsible for setting and administering procedures for the management and security of donor personal and financial information. Security practices for HHs' Client Record Management (CRM) and payment applications used for processing credit card donations are consistent with HHs' Information Management and Security policy and include:

1. Each user shall be assigned a unique login identification (ID)
2. A unique password shall be assigned to a user upon access approval. The password may be updated by the user within define CRM password specifications
3. User login IDs may be audited, and all inactive login IDs shall be terminated by the CRM HHs' administrators (currently the CDO and the FDC).
4. The login ID is locked or revoked after a maximum of three (3) unsuccessful login attempts which then require the passwords to be reset by the appropriate Administrator

B. Donor Information: Donor's contact information is entered and held in HHs' CRM consistent with the Fund Development procedure, Gift Entry-CRM Procedure. Information entry and access is restricted to approved Fund Development Staff.

1. HH restricts the use of donors' personally identifying information to communicating with donors, processing donations and for donor recognition. HH does not disclose or share donor information except when we have donor permission or as required by law. Internal use of donor information is restricted to HHs' Chief Executive Officer (CEO),

CDO, Fund Development Staff (and volunteers), Board members and HHs' printer and mailing providers.

2. HH uses third party providers to assist with processing and managing donations and donor information. Our providers have access to donor information under strict confidentiality rules and are permitted to use donor information only to support HHs' operations. The third-party providers are responsible for ensuring data and information security including monitoring for system breaches.

C. <u>Credit Card Payments and Information:</u> HH uses a third party provider to enter and process credit card donations. Donor credit card security is administered consistent with the Payment Card Industry Data Security Standard (PCI DSS) Program. All employees are required to adhere to the policies described herein.

1. Scope of Compliance: The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, HHs' credit card processing environment consists of smartphone readers, data entry directly to the CRM and website access. HHs stores limited credit card information on its CRM including donor XXX.
2. Prohibited Data: HH staff shall delete and/or destroy any recorded sensitive authentication data post-authorization so that data is unrecoverable. The following information shall not be stored after authorization (even if encrypted):
    - The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)
    - The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)
    - The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)
    - HH shall mask the display of donor credit card primary account numbers (PAN), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show no more than the first six and the last four digits of the PAN. (PCI requirement 3.3)
3. Transmission of Cardholder information: HH staff are prohibited from sending unencrypted PANs through messaging technologies including but not limited to text, email, chat, etc. (PCI requirement 4.2)
4. Access to Cardholder Information: Access to HHs' cardholder system components and data is limited to individuals whose jobs require such access. (PCI Requirement 7.1) Access limitations must include the following:
    - Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.2)
    - Privileges are assigned to individuals based on job description and function (also called "role-based access control). (PCI Requirement 7.1.3)
    - Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) shall be physically secured (PCI requirement 9.5) and maintained with strict control over internal or external distribution of any kind of documents containing cardholder data
    - All documents containing cardholder data shall be destroyed when no longer needed for business or legal purposes (PCI requirement 9.8), documents shall be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. (PCI requirement 9.8.1.a) Containers storing information waiting to be destroyed must be secured (locked) to prevent access to the contents by unauthorized personnel. (PCI requirement 9.8.1.b)

5. Payment Devices: Devices that capture payment card data via direct physical interaction with the card (such as swipe/chip readers and any other payment terminals) shall protected including but not limited to, preventing the devices from being tampered with or substituted. (PCI requirement 9.9). HH shall maintain an up-to-date list of devices. Employees shall be instructed to maintain the integrity and currency of the inventory. The list should include the following: (PCI requirement 9.9.1)
    - Make and model of all devices
    - Location of each device (for example, the address of the site or facility where the device is located)
    - Device serial number or other method of unique identification
    - The payment devices must be periodically inspected. Check surfaces to detect tampering (for example, addition of card skimmers to devices). Checks must also be made that will detect substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). (PCI requirement 9.9.2)

   Employees, volunteers and contractors who interact with the payment devices shall be provided with training that enables them to be aware of attempted tampering or replacement of devices. Training shall include the following: (PCI requirement 9.9.3)
    - Verify the identity of any third-party persons claiming to be repair or maintenance personnel prior to granting them access to modify or troubleshoot devices
    - Employees must be instructed not to install, replace, or return devices without verification from management. The inventory list (required previously) must be updated by the employee when device locations are changed or new devices are added.
    - Employees need to be aware of suspicious behavior around devices (for example, attempts by unknown or unauthorized persons to unplug or open devices).
6. Credit Card Information Security Incident
    - Incident Identification: Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular area of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to:
        - Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry).
        - Fraud – Inaccurate information within databases, logs, files or paper records.
    - Reporting and Incident Response: The CEO shall be notified immediately of any suspected or real security incidents involving cardholder information. No HH employee shall communicate with anyone outside of their supervisor(s) or the CEO regarding the details or generalities surrounding any suspected or actual cardholder information incident. All communications with law enforcement, card holders, or the public shall be coordinated by the CEO.

Communication and Training:

The Board shall receive a copy of the policy at the time of periodic review and will have an opportunity to ask clarifying questions during the approval process. Employees and volunteers shall receive notice of the Board's policy review and approval including notice of any substantive changes. The notice will provide a link to the policy located on the HH website.

Fund development staff shall receive training on this policy, related procedures and the required technology as part of initial orientation and as updates are made to technology applications or providers.

Definitions:

1. Client Relationship Manager: A database system used for donor and gift information and relationship management.

2. Payment Card Industry Compliance: Standards and business practices that help ensure the security of each one of your business's credit card transactions.

3. Personally Identifying Information: Information about an individual that may directly or indirectly identify that individual. Personally identifying information includes information such as an individual's name, address, other contact information, race, birth date, financial or payment information, etc. Personally identifying information also may include information that is encoded, encrypted, hashed, or otherwise protected.

Other Related Materials:

Processing Credit Pard Donations Procedure

References/Legal Authority:

Best Practice for Maintaining PCI DSS Compliance, 2019.

Compliance Guide for Tax Exempt Organizations, Internal revenue Service, 2023.

Change Log:

Date of Change	Description of Change	Responsible Party
02.2024	This is a new policy.	E. Hall, CDO and K. Fitzgibbons, FDC