Chapter:	Technology and Facilities Management		
Title:	Information Management and Security		
Policy: ☒ **Procedure:** ☐	**Review Cycle:** Triennial **Author:** DO	**Adopted Date:** 03.2024 **Review Date:** 03.2024	**Related Policies:** Agency Property Confidentiality and Privacy Donor Information Privacy & Security Standards of Conduct Electronic Communication and Internet Use Telecommuting and Remote Work

Purpose:

Hopeful Horizons (HH) has adopted this policy to establish and clarify its technology management and security practices and expectations.

Scope:

This policy applies to:

☒ All HH Staff ☐ Selected HH Staff, as specified:

☐ HH Board Members ☒ HH Volunteers

☒ Other: Contractors assigned HH technology equipment or with data access

Policy:

HH shall administer information technology systems and related data consistent with the requirements established in this policy to:

- Protect the integrity and quality of retained/stored information/data
- Ensure the confidentiality of client, employee, volunteer and donor information
- Support risk management strategies
- Protect HHs' investment in technology

This policy includes the management of all types of paper and electronic information maintained by HH including:

- Case records and other information of persons served
- Administrative, financial, and risk management records and reports
- Personnel files and other human resources records
- Performance and quality improvement data and reports

A. Technology Assessment: HH shall annually assess its technology and information management needs including a review of:

- Efficacy of current technology and information systems in use by the organization
- Short- and long-term goals for utilizing technology
- Effectiveness of technology and data security systems and practices
- Information technology contractor performance
- Current technical skills of staff and need for staff training

B. General Requirements: Employees and volunteers are responsible for proper care and use of HHs' provided technology and the protection and security of all data/information that may come to them or to which they have access.
    1. Identify, intervene with and as necessary report unrecognized persons in restricted areas of HHs' facilities
    2. Unattended computers shall be screen lock password protected by the user when leaving the work area
    3. Only computer hardware and software owned, leased or subscribed to and installed by HH is permitted to be connected to or installed on organization equipment.
    4. Personal computers supplied by HH are to be used solely for business purposes
    5. Modifications or configuration changes are not permitted on HH computers
    6. All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of HH are the property of HH unless covered by a contractual agreement
    7. Nothing contained herein applies to software purchased by employees at their own expense

C. Prohibited Activities: HH Employees and volunteers are prohibited from engaging in any activity that could lead to damage, destruction or loss of technology equipment or its associated data including but not limited to:
    1. Deliberately crashing an information system. Users may not realize that they caused a system crash, but if it is shown that the crash occurred because of user action, a repetition of the action by that user may be viewed as a deliberate act
    2. Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs and attempting to circumvent file or other resource permissions
    3. Introducing, or attempting to introduce, computer viruses or other malicious code into an information system
    4. The willful, unauthorized access or inspection of confidential or sensitive information to which the user has not been approved is prohibited
    5. Violating or attempting to violate the terms of use or license agreement of any software product used by HH
    6. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of HH

D. User Identification and Authentication: HH shall establish and maintain a secure user identification (ID) and authentication system for approved access/use of its technology equipment and data systems. HH and/or its contractor(s) shall maintain an access control system that identifies each user and prevents/monitors unauthorized access. Security requirements for user identification 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 is configured consistent with Microsoft guidelines and may only be updated by the technology support provider
    3. Users are responsible for the security and use and misuse of their individual logon ID and password. Users are expressly prohibited from sharing their unique user ID and/or password
    4. User login IDs may be audited, and all inactive login IDs shall be terminated

5. 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 technology support provider

Upon termination of an employee/volunteer/contractor, whether voluntary or involuntary, HR or the DO shall promptly notify the technology support provider to terminate all accesses. If the employee's termination is voluntary and employee provides notice, HR or the DO shall promptly notify the technology support provider of employee's last scheduled workday so that their user account(s) can be configured to expire. The employee's supervisor or department head shall be responsible for insuring that all technology devices and HH equipment are returned to the organization prior to the employee leaving on their final day of employment in accordance with HHs' Agency Property Policy

E. Access Controls: HH electronic client records (ECRs) are protected by additional use of access control systems to assure appropriate access to protected client information. Rules for access to the ECR have been established by HHs' Chief Executive Officer (CEO)/designee. Users may be added to the ECR only upon their supervisor's approval. The supervisor shall define the requirements within which the employee may access data/information.

F. Transfer of Sensitive/Confidential Information: All employees must recognize the sensitive nature of data maintained by HH and hold all data/information in the strictest confidence. When confidential or sensitive information from one individual is received by another individual while conducting official HHs' business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual/organization and HHs' Confidentiality and Privacy policy.

   In accordance with the Health Insurance Portability and Accountability Act (HIPAA), all personally identifying information shall be removed from all data that falls within the definition of protected health information (PHI) before it is exchanged. HH does not transfer health records with restricted personally identifying information electronically.

G. Contingency Plans: HH shall adopt policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain personally identifying (PII) and/or protected health information (PHI). HH shall continually assess potential risks and vulnerabilities to PII and PHI in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule. Procedures shall be practiced for data back-up and disaster recovery and emergency mode operations.

H. Policy Violations: Violations of this policy including any improper use of HH provided technology equipment are subject to discipline up to and including discharge.

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.

New employees shall review this policy and any related procedures as part of their initial orientation.

Definitions:

1. Electronic Client Record: An ECR is a digital version of a client's paper record. ECRs are real-time, client-centered records that make information available instantly and securely to authorized users. HHs' uses Collaborate as its ECR.

2. Personally Identifying Information: Information about an individual that may directly or indirectly identify that individual. In the case of a victim of domestic violence, dating violence, sexual assault, or stalking, it also means information that would disclose the location of that individual. Personally identifying information includes information such as an individual's name, address, other contact information, and social security number, but it also can include information such as an individual's race, birth date, or number of children if, in the particular circumstances, that information would identify the individual. Personally identifying information also may include information that is encoded, encrypted, hashed, or otherwise protected.

3. Protected Health Information: Individually identifiable health information is information, including demographic data, that relates to:
   - ✓ the individual's past, present or future physical or mental health or condition,
   - ✓ the provision of health care to the individual, or
   - ✓ the past, present, or future payment for the provision of health care to the individual, and
   - ✓ that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

4. Technology Equipment: technology assets including mainframe computers, servers, general computer equipment, printers, monitors, hard drives, memory and storage devices.

5. Technology Support Provider: HH contracts with a third party for technology support, system back-up and information storage.

Other Related Materials:

Technology Support and Network Administration Contracts
Information Back-up and Contingency Plan Procedure
Information and Technology Problem Solving Procedure
Emergency Access to Protected Health Information Procedure
Electronic Communication and Internet Use Procedure
Telecommuting and Remote Work

References/Legal Authority:

Technology and Information Management, Risk Prevention and Management Standards (RPM) 4, Council on Accreditation, 2023.

Change Log:

Date of Change	Description of Change	Responsible Party
3.2024	This is a new policy	N. Miller, Prog. Eval. Consultant in consultation with J. Brown, Dir of Operations