DATA SECURITY POLICY

This Data Security Policy is intended to document our policies and procedures for safeguarding all Sensitive and Confidential Data found on records and in systems owned by us.

Confidential data is defined below and includes protected health information (PHI) and personally identifiable information (PII) as defined in our Internal Privacy Policy. This policy is maintained under the care custody and control of the YMCA to facilitate compliance with applicable laws and regulations on the protection of Sensitive and Confidential Data.

Effective Date: 12/04/2017
Category: SECURITY
Y-USA Template V.12.10.14

Contact(s):
Nathan Prenzlow
CEO
712-262-3782
nprenzlow@spencerymca.org

1.0 OVERVIEW

Spencer Family YMCA is committed to protecting the confidentiality of all Sensitive and Confidential Data that our organization, or individuals or companies acting on our behalf, maintain(s). This includes information about our own employees (full-time and part-time), our constituents (members, volunteers, donors), and our associates (third- party vendors and contractors). Accordingly, we have implemented a number of data security policies and procedures to protect such information.

Read this Data Security Policy in conjunction with the documents that are cross-referenced in Section 6 below.

In accordance with federal and state laws and regulations, our organization may be required to take measures to safeguard Sensitive and Confidential Data, and to provide notice about security breaches of Sensitive and Confidential Data as outlined in our Data Security Incident Response Plan to affected individuals and appropriate state agencies.

2.0 PURPOSE

The purposes of this document are to

- establish a comprehensive data security program for our organization, with policies and procedures to safeguard Sensitive and Confidential Data that is maintained by us or on our behalf, in compliance with federal and state laws and regulations;
- establish staff and volunteer responsibilities in safeguarding Sensitive and Confidential Data according to its classification level; and
- establish reasonable and appropriate administrative, technical, and physical safeguards to protect the security of Sensitive and Confidential Data.

3.0 SCOPE

This Policy applies to all employees, whether full- or part-time, permanent or temporary, and interns (hereinafter "Employees"). It also applies to volunteers, contractors, or other third parties who have access to the covered data.

The data covered by this Policy includes any Sensitive and Confidential Data stored, accessed, or collected by or on behalf of our organization. The Information Security Policy is not intended to supersede any existing policies that may contain more specific requirements for safeguarding certain types of information.

3.1 Definitions

For purposes of this Plan, **"Sensitive and Confidential Data"** is defined as an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to that individual:

- Social Security number
- Driver's license number or state-issued identification card number
- Financial account number or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to that individual's financial account
- Information created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, that relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual

However, **Sensitive and Confidential Data does not include** information that is lawfully obtained from public domain or from federal, state, or local government records lawfully made available to the general public.

3.2 Data Classification

All data covered by this Data Security Policy falls into one of three categories, outlined below.

Public (or Unrestricted): Public (or Unrestricted) information includes any information for which there is no restriction to its distribution and where the loss or public use of such data would not present any harm to our organization or our constituents. Any data that is not classified as Sensitive or Confidential as defined below should be considered public data.

Sensitive (or Restricted): Sensitive or Restricted data refers to any information where unauthorized access, use, alteration, or disclosure could present a moderate level of risk to our organization. Access to this data should be limited to individuals who are employed by our organization and who have legitimate reasons for accessing such data. Any nonpublic information that is not explicitly designated as Confidential should be treated as Sensitive data. A reasonable level of security should be applied to this classification to protect the privacy and integrity of this data.

Confidential: Confidential data refers to any data where unauthorized access, use, alteration, or disclosure of this data could present a significant level of risk to our organization or our constituents. Confidential data should be treated with the highest level of security to protect the privacy of the data and prevent any unauthorized access, use, alteration, or disclosure.

Confidential data includes any information that is protected by federal or applicable state laws or regulations, including, but not limited to, data protected under the following privacy laws: Health

Insurance Portability and Accountability Act of 1996 (HIPAA), Family Educational Rights and Privacy Act (FERPA), and the Federal Trade Commission's Red Flag Rules.

Confidential data also includes other sensitive personal and institutional or company data where the loss of such data could harm an individual's right to privacy or negatively impact the finances, operations, brand or reputation of our organization or our constituents. This data includes, but is not limited to, constituent information, intellectual property, financial and investment records, employee salary information, or information related to legal or disciplinary matters.

4.0 POLICY

4.1 Responsibilities

All Sensitive and Confidential Data that our organization collects or accepts makes us a "data owner." Data owners are responsible for approving who will have access to such data.

Human Resources will inform appropriate personnel about a staff person's change of status. Changes in status include terminations, leaves of absence, significant changes in position responsibilities, transfer to another department, or any other change that might affect a staff person's access to data. HR staff, in conjunction with the Information Technology Department will inactivate all of the staff person's account access upon termination date.

Persons who have access to data by virtue of a contract (vendors, contractors, etc.) are permitted only the degree of access provided for in the contract. At the conclusion of the contract, their access rights will terminate and the Information Technology Department will inactivate access. Member Services is responsible to verify such access rights have been terminated and inactivated.

The Member Services will take reasonable steps to monitor systems for unauthorized use of or access to data. These actions will include (as appropriate, but are not limited to) detecting intrusion, maintaining application and network security logs, reviewing server firewall for security vulnerabilities, and performing file system audits.

All Employees are responsible for maintaining the privacy and integrity of all sensitive and confidential data as defined above and must protect the data from unauthorized use, access, disclosure, or alteration. All are required to access, store, and maintain records containing sensitive and confidential data in compliance with this Policy and will notify appropriate department personnel of any suspected violation, whether willful or through negligence, of the policy.

4.2 Identification and Assessment of Risks to Confidential Data

Our YMCA recognizes that there are both internal and external risks to the privacy and integrity of Sensitive and Confidential Data. These risks include, but are not limited to, the following:

- Unauthorized access of Sensitive and Confidential Data by someone other than the owner of such data
- Compromised system security as a result of system access by an unauthorized person
- Interception of data during transmission
- Loss of data integrity
- Physical loss of data in a disaster
- Errors introduced into the system
- Corruption of data or systems
- Unauthorized access of Sensitive and Confidential Data by employees

- Unauthorized requests for Sensitive and Confidential Data
- Unauthorized access through hard copy files or reports
- Unauthorized transfer of Sensitive and Confidential Data through third parties

We recognize that this may not be a complete list of the risks associated with the protection of Sensitive and Confidential Data. Since technology growth is not static, new risks are created regularly. Accordingly, these and other safeguards are designed to protect against currently anticipated threats or hazards to the integrity of such information. IT Risk Assessments are periodically reviewed, updated annually, and maintained electronically by authorized staff and individuals.

4.3 Policies for Safeguarding Sensitive and Confidential Data

To protect Sensitive and Confidential Data, we have developed the following policies and procedures relating to collection, access, storage, transportation, and destruction of records.

Collection

- Collection of Sensitive and Confidential data should be for current and specific documented business purposes only and not for possible future use or any other ancillary reason.

Access

- Only those Employees requiring access to Sensitive and Confidential Data in the regular course of their duties are granted access to Sensitive and Confidential Data, including both physical and electronic records. Computer and network access passwords are disabled upon termination of employment. Upon termination of employment, physical access to documents or other resources containing Sensitive and Confidential Data is immediately prevented.

Storage

- Employees will not store Sensitive and Confidential Data on unencrypted laptops or on other mobile devices (e.g., flash drives, smart phones, and external hard drives). In rare cases where it is necessary to transport Sensitive and Confidential Data electronically, the mobile device containing the data must be encrypted.
- To the extent possible, all Sensitive and Confidential Data must be stored only on secure servers maintained by the organization and not on local machines, unsecure servers, or portable devices.
- Paper records containing Sensitive and Confidential Data must be kept in locked files or other secured areas when not in use.
- Electronic records containing Sensitive and Confidential Data must be stored on secure servers and physically located in a secure location, and, when stored on authorized desktop computers, must be password protected.

Taking Records Off-Site

- Employees are strongly discouraged from removing records containing Sensitive and Confidential Data off-site. In rare cases where it is necessary to do so, the user must take all reasonable precautions to safeguard the data. Under no circumstances are documents, electronic devices, or digital media containing Sensitive and Confidential Data to be left unattended in any insecure location.
- When there is a legitimate need to provide records containing Sensitive and Confidential Data to a third party, electronic records shall be password-protected and/or encrypted, Confidential Data electronic records shall be encrypted, and paper records shall be marked confidential and securely sealed.

Destruction of Sensitive and Confidential Data

- Follow the organization’s records retention and destruction policy for destruction of paper and electronic records containing Sensitive and Confidential Data. Paper records must be

destroyed in a manner that prevents recovery of the data, such as using a Security Micro Cut Shredder.

4.4 Third-Party Vendor Agreements Concerning Protection of Personal Information

We exercise appropriate diligence in selecting service providers capable of maintaining appropriate security safeguards for Sensitive and Confidential Data provided by us to them. The primary director for each department is responsible for identifying those third parties providing services that have access to Sensitive and Confidential Data. All relevant contracts with these third parties are reviewed and approved by the CEO to ensure the contracts contain the necessary flow-down or other language requiring such third parties to safeguard our Sensitive and Confidential Data. It is the responsibility of the director to confirm that the third parties are required to maintain appropriate security measures in order to protect Sensitive and Confidential Data consistent with this Policy. All vendors and other third parties should complete a Security Questionnaire or similar risk assessment that demonstrates their ability and commitment to protecting our Sensitive and Confidential Data.

4.5 Computer System Safeguards

Northwest Communications monitors and assesses information safeguards on an ongoing basis to determine when enhancements are required. We have implemented the following to combat external risk and to secure the network and data containing Sensitive and Confidential Data:

- Protocols are used for validating the authentication of secure users.
- Unique passwords are required for all user accounts.
- Each employee receives an individual user account.
- Server and user accounts are locked after multiple unsuccessful password attempts.
- Computer access passwords are disabled upon an employee's termination.
- User passwords are stored in an encrypted format.
- Root passwords are accessible only by system administrators.
- Secure access control measures (access to specific systems containing Sensitive and Confidential Data) are in place and limited to those Employees who require such access in the normal course of their duties.
- Each person who has access to our system has been assigned unique credentials for the computer network. The employee, volunteer, or associate who, in the course of his or her duties, needs to obtain access to any system that contains Sensitive and Confidential Data must use these unique credentials.
- Files containing Sensitive Data transmitted outside of the network are to be password protected and/or encrypted. Files containing Confidential Data transmitted outside of the network are to be encrypted.
- Northwest Communications performs regular internal network security audits to all server and computer system logs to discover, to the extent reasonably feasible, possible electronic security breaches and to monitor the system for possible unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Sensitive and Confidential Data.
- All computers and servers are firewall protected and regularly monitored.
- Operating system patches and security updates are installed to all servers as needed.
- Antivirus and antimalware software is installed and kept updated on all servers and workstations.
- Virus definition updates are installed on a regular basis, and the entire system is tested and checked at each installation.

4.6 Employee Training

All Employees who have access to Sensitive and Confidential Data are required to read and accept this Security Policy and complete annual training on information security to understand their responsibilities related to this Policy. The training is also strongly recommended for ALL Employees. The HR Department maintains records of all such training. All Employees should

expect to receive additional training materials, security reminders, and a security refresher on a regular basis.

4.7 Reporting Attempted or Actual Breaches of Security

Any incident of possible or actual unauthorized access to or disclosure, misuse, alteration, destruction, or other compromise of Sensitive and Confidential Data, or of a breach or attempted breach of the information safeguards adopted under this Policy, must be reported immediately to the CEO. The CEO is charged with the identification of all data security incidents where the loss, theft, unauthorized access, or other exposure of sensitive or confidential data is suspected. The HR Department will document all breaches and subsequent responsive actions taken.

For more information about incident response, including specific procedures for responding to a breach, see our Data Security Incident Response Plan, available upon request.

5.0 ENFORCEMENT

Any employee who willfully accesses, discloses, misuses, alters, destroys, or otherwise compromises information classified as Sensitive or Confidential without authorization, or who fails to comply with this Policy in any other respect, will be subject to disciplinary action, which may include termination and legal ramifications.

6.0 POLICIES OR PROCEDURES CROSS-REFERENCED

The following Security Policies and Procedures provide advice and guidance that relates to this Policy:

- Spencer Family YMCA Internal Privacy Policy
- Spencer Family YMCA External Privacy Policy
- Spencer Family YMCA Data Security Incident Response Plan

This policy is subject to change or can be terminated by the Company at any time. This policy ***supersedes*** all prior policies, procedures, or advisories pertaining to the same subject.

Policy Revision History			
Version:	**Effective Date:**	**Authorized by:**	**Affected Provisions:**
Version 0.1	12/04/2017	**Nathan Prenzlow**	**--**