FOR YOUTH DEVELOPMENT®
FOR HEALTHY LIVING
FOR SOCIAL RESPONSIBILITY

DATA SECURITY INCIDENT RESPONSE PLAN

Spencer Family YMCA is committed to the security of its sensitive and confidential information. However, even with the most reasonable precautions, data security incidents may occur. This plan provides guidance on (1) planning for, and (2) responding to data security incidents, including data breaches involving protected personal information. It includes the designation of an individual, under the direction of internal or outside legal counsel, to respond to suspected and actual data security incidents.

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

SCOPE

This plan applies to data security incidents involving protected personal information or sensitive data, such as trade secrets or other confidential information, held by our YMCA or associates working on behalf of our YMCA.

All employees (full-time and part-time), associates (third-party vendors and contractors) and volunteers that collect, store, or otherwise process or have access to protected personal information are included in the scope of this plan.

Nathan Prenzlow, CEO, is further responsible for the annual review and update of this plan and for the consideration of any necessary changes in the wake of a data security incident.

1.0 DEFINITIONS

Confidential Information: Sensitive data, such as trade secrets, business plans, internal reports, or other nonpublic corporate information, as well as other confidential data, including information regarding YMCA constituents (members, volunteers, donors).

Constituents: Persons included in the data we collect, such as employees, members, volunteers, donors, contractors, vendors, etc.

Data Security Breach: Malicious or purposeful circumvention of IT controls or gaining unauthorized access.

Data Security Incident: Any action or event of significant risk that may lead to or directly results in an attempt to circumvent IT controls or gain access to data that is not authorized.

Incident Response Contact or Group: The individual or group that is ultimately responsible for the management of this Plan. The Incident Response Contact is Megan Whittaker, Director of Operations, 712-262-3782.

PCI DSS: The Payment Card Industry Data Security Standards. The largely contractual information security requirements for those who store, process, or transmit payment card information that are enforced by payment card issuers, such as VISA and MasterCard.

Personal Information: Information that can be used to distinguish or identify an individual, such as his/her name, contact information including home or email address, Social Security number, date of birth, credit card or payment card information, or any other sensitive nonpublic personal information that is linked or linkable to a specific individual or could subject him/her to identity theft. Personal Information may relate to constituents, employees, or any other associate as defined below.

2.0 ELEMENTS OF THE INCIDENT RESPONSE PLAN

- **Report.** Immediately report any Data Security Incident or Data Security Breach.
- **Contain.** Promptly investigate the incident and take necessary steps to end or minimize further data loss or compromise.
- **Classify.** Classify the incident and notify key internal stakeholders.
- **Preserve.** Document the incident and safeguard relevant information.
- **Assess.** Assess impact and required next steps and follow-up actions.
- **Notify.** Determine and implement required notification(s).
- **Recover.** Recovery, record keeping, and review.

3.0 INCIDENT RESPONSE PLAN

3.1 Report

Any employee who becomes aware of a Data Security Incident or Data Security Breach must immediately report his or her concerns to the Incident Response Contact, as well as to his or her immediate supervisor.

- The Incident Response Contact may be contacted at 712-262-3782.
- If the Data Security Incident or Data Security Breach occurs outside of regular business hours and the above contact is unavailable, contact Megan Whittaker, Director of Operations, at mwhittaker@spencerymca.org.

Upon notification of a suspected or confirmed incident, the Incident Response Contact should immediately gather as much information as possible from the individual reporting the incident.

The reporting individual must immediately open an incident report and immediately record all pertinent information (see Exhibit A); the reporting individual should also provide the requested information based only on known and confirmed facts, to the best of his/her ability, at the time of the report.

Individuals reporting a Data Security Incident or Data Security Breach shall take direction from the Incident Response Contact regarding next steps in compliance with this Policy and shall support the investigation, mitigation, and recovery activities as needed.

3.2 Contain

Immediately upon detecting a Data Security Incident or Data Security Breach, steps must be taken to contain the incident and secure the data.

Example containment scenarios:

Confidential Data Exposure
- Disable all access to the application, the website, and the server as soon as the exposure is discovered or the disclosure made.
- Do not turn off the server, as key and critical forensic data that is crucial to the investigation may be lost.

Criminal Activity
- Secure the facility, prioritize the safety of individuals.
- Call 911 if anyone is seriously injured or in the event of an emergency.
- Notify building security and/or local law enforcement.

Denial of Service (Service is blocked and the YMCA cannot get service.)
- Contact ISP (Internet service provider) and notify it of the denial of service.
- Block WAN (wide area network) traffic or disconnect router from WAN.

Malicious Code
- Disconnect infected machine from LAN (local area network) or disconnect all machines from LAN (disconnect switch from patch panel workstations are connected to).

Policy Violation
- Varies depending on situation. Consult Megan Whittaker, Director of Operations, at 712-262-3782.

Unauthorized Information Disclosure
- Protect information from further disclosure.
- Notify sender and, if applicable, the intended recipient per federal and state laws and regulations. Additionally, seek legal counsel to ensure the requirement for and appropriateness of notifications.

No Incident Determined (False Alarm)
- No action required.

3.3 Classify

Data Security Breaches will be classified by the Incident Response Contact or Group according to incident categories and severity. Incident response will be based on classification. A single incident may have several categories.

Below is a list of classifications. Examples in categories are not meant to be exhaustive.

Confidential Data Disclosure
- Social Security numbers (with or without names)
- Credit Card numbers
- Protected health information (any form; electronic or print)
- Employee data and/or company trade secrets
- System exploit/compromise
- Other

Criminal Activity/Investigation
- Subpoena, search warrant, or other court order
- Litigation hold request (e-discovery)

- Online theft, fraud
- Physical theft, break-in
- Other

Denial of Service
- Single or distributed (DoS or DDos)
- Inbound or outbound

Malicious Code
- Worm, virus, Trojan
- Botnet
- Keylogger
- Rootkit
- Other

Policy Violation
- Password sharing
- Failing to protect sensitive / confidential information
- Improper use of system or information handling
- Unauthorized access or non-permitted use of resources
- Other

No Incident
- False positives as may be detected by the following:
  - Internal/External security vulnerability and baseline security scans
  - Log file reviews
  - Monitoring
  - When investigation of suspected and/or reported activity finds no evidence of an incident
  - Others

3.4 Preserve
Document and preserve evidence.

Immediately begin detailed investigation of the incident and thoroughly review document. The key is to be able to identify at a detailed level the situation that occurred, how and/why it occurred, and the impact of the incident in terms of loss, disclosure, destruction, outage, etc.

3.5 Assess
Assess and determine conclusions. (Ideally within 24 hours)

- After initial notification, the Incident Response Contact or Group will perform a more thorough analysis to consider the factors listed below. Depending on the size and scale of the incident, internal or outside legal counsel should be involved when appropriate given the significance of the potential risk to the YMCA and to the individuals whose Personal Information may be affected by the Data Security Incident or Data Security Breach. Factors to consider include
  - what resources are needed for escalation, mitigation, and remediation;
  - whether misuse of data is reasonably likely;
  - whether any trades secrets or other confidential information was compromised;
  - whether law enforcement should be contacted;
  - whether independent forensic analysis should be pursued, including whether PCI DSS obligations require engagement by a Payment Card Industry Forensic Investigator;
  - if internal legal counsel is handling, whether outside legal counsel should be engaged;

- whether separate PR assistance should be engaged;
- whether the YMCA's insurance carriers should be notified and the policy timeline for reporting should be initiated;
- what level of notification is appropriate to affected individuals, credit card companies or issuing banks, and/or regulators, including whether to establish a web page and/or a toll-free telephone number;
- options for mitigating the risk, including technical solutions, as well as offers of credit monitoring; and
- whether to seek compensation or other legal recourse against any responsible third party.

- The following analysis may be conducted by legal counsel:
  - Determine litigation risks related to Data Security Incident or Data Security Breach.
  - Determine whether any other obligations stem from relevant agreements or privacy policies.
  - Identify the legal jurisdictions involved (determined by the location and residence of affected individuals and systems).
  - Identify state data breach statutes involved, recognizing that the relevant law is the law of the state where the people reside, not where the YMCA is located. For a generally accurate listing of the laws, go to the Security Breach Notification Laws page of the National Conference of State Legislatures at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.
  - Determine whether there is insurance coverage that applies to the Data Security Incident or Data Security Breach.
  - Determine the liability risk of individual employees, including whether employees violated internal policies or laws.
  - Determine whether there may be liability on the part of any other third party.

- Consult state law for notification requirements. In addition to the specific requirements of applicable law, the YMCA may, in its discretion, consider providing voluntary notification.
  - If the Data Security Incident or Data Security Breach involves information that could potentially lead to access to an individual's banking, credit card, or other personal financial information, such as an account name and password, YMCA shall notify the individuals and inform them of steps that they should take to mitigate the risk.
  - If the Data Security Incident or Data Security Breach involves payment card information, YMCA should notify the issuing banks or credit card companies promptly.

- Help Line. If the Data Security Incident or Data Security Breach involves a large volume of individuals' personal information, consider establishing a toll free help line that allows affected users to call for more information.

  Note: Breach notification, and the responses it generates, can lead to significant tangible and intangible costs. Costs can include the costs to the YMCA in facilitating the actual notification and/or offers for credit monitoring; and fees for professionals required to appropriately communicate with regulators, media members, and affected individuals. There may also be brand and reputational costs inherent in publicizing a Data Security Incident or Data Security Breach. Additionally, there are external costs, including the financial expense and inconvenience to affected individuals for canceling credit cards, closing bank accounts, placing fraud alerts on credit files, and/or obtaining new identity documents.

  Repeated events can cause notice fatigue and undermine the effectiveness of breach notification in mitigating serious threats. Careful consideration must be taken so that the incident response, including notification, is commensurate with the practical risks of the Data Security Incident or Data Security Breach.

3.6 Notify

The Incident Response Contact or Group, under leadership and with guidance from legal counsel, must determine whether notice to law enforcement, regulators, credit reporting agencies, business partners, and affected individuals is required or otherwise appropriate. In making this determination, the Incident Response Contact or Group should review all applicable state data breach laws, which can be found at the Security Breach Notification Laws page of the National Conference of State Legislatures at www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. If legal counsel determines that notification is required, the following elements should be incorporated into the notification process:

A. Timing of Notification

Notice should be provided in the most expedient time possible and without unreasonable delay, after determining the full scope of affected data, the causes of the Data Security Incident or Data Security Breach, and the immediate steps necessary to address the breach and mitigate damage. Notification based on premature or incomplete facts or in a manner likely to make identity theft more likely to occur as a result of the announcement undermines the purpose of the notifications.

Additionally, if a Data Security Incident or Data Security Breach requires assistance from law enforcement, the Incident Response Contact or Group should confirm with law enforcement that notification to affected individuals would not impede the ongoing investigation. If law enforcement requests that notification be delayed, obtain this request (or confirm the request) in writing and maintain this record as a part of the Data Security Incident Report Form.

In the event that regulators must be notified, the Incident Response Contact or Group must coordinate regulator notice to be provided before, or at least simultaneously, with notification to affected individuals.

Notification to credit card companies pursuant to PCI DSS requirements requires legal review of contractual obligations. Generally, in addition to the immediate notification to credit card companies and issuing banks where there is suspected or confirmed loss or theft of credit card data, written documentation of the initial investigation will likely be required to the credit card companies within three (3) business days.

B. Notification Source

Notification to law enforcement, regulators, credit reporting agencies, business partners, and affected individuals must be managed and issued by the internal or outside legal counsel, which will analyze notification obligations based on applicable law.

Where a Data Security Incident or Data Security Breach involves a service provider, the source of the notice to affected individuals may appropriately come from that service provider. But in all cases, notification by a service provider must be coordinated with the Incident Response Contact or Group.

A communications strategy for additional communications regarding the Data Security Incident or Data Security Breach, such as responses to media inquiries or follow up questions from affected individuals or business partners, must be in place prior to notification. Inquiries from regulators must be handled directly by the internal or outside legal counsel.

C. Notification Content

Notice should be reduced to a stand-alone document and written in clear, concise, and easy-to-understand language. The content of notification letters are subject to varying state law requirements. Accordingly, the final content of notification must be approved by internal or outside legal counsel. The Sample Security Breach Notification Letter provides an example of a notification letter.

The notice should include

- a brief description of what happened;
- a description of the types of data involved (e.g., names, passwords, credit card numbers, etc.);
- what the YMCA has done to investigate, mitigate damage, and protect against further incidents;
- contact procedures for those wishing to ask questions or learn additional information, including a toll-free telephone number, website, and/or postal address; and
- steps individuals should take to protect themselves from the risk of identity theft.

D. Method of Notification

Notification should be provided in written format to the last known mailing address of the individual. Returned mailings should be run through a national change of address vendor and re-mailed if a new address is obtained.

Substitute means of notice, such as through electronic notice to email addresses and/or through posting on the YMCA's website, may be considered for voluntary breach notifications, particularly for breaches that are low risk.

If there is no physical mailing address on record, the affected individual has provided an email address for communication purposes, and the affected individual has consented to use of the email address as a primary means of communication, notification by email may be appropriate for required breach notification as well.

Certain government regulators require notice to be provided in a specific form, such as through an online intake or accompanying reporting form. Regulator notice must be provided as specified under applicable law or regulatory guidance, which shall be confirmed by internal or outside legal counsel.

In addition to the notification letter, the Incident Response Contact or Group may wish to develop supplemental materials to handle member or media inquiries, including preparation of a call script, a press release, and/or frequently asked questions. Such supplemental materials could also be posted on the website.

3.7 Recover

Recovery, record keeping, and review. At the conclusion of a Data Security Incident or Data Security Breach, the Incident Response Contact or Group shall do the following:

A. Finalize the risk assessment and internal investigation, including determination of the root causes of the Data Security Incident or Data Security Breach.

B. Maintain records of the YMCA's incident response for a minimum of 5 years, including:

- Supplement or complete the Data Security Incident Report and all other reports and materials and communications developed to respond to the Data Security Incident or Data Security Breach.
- Maintain copies of records of notifications, including all correspondence with affected individuals, regulators, or other third parties.
- Maintain a database of the addresses used to contact any affected individual, as well as a record of all returned mailings, along with the date of return.

C. Prepare for litigation:

- Assess potential for civil litigation against the YMCA, whether by affected individuals or third parties seeking indemnification.
- Assess whether there are claims against third parties that should be pursued.
- Issue litigation holds as necessary and appropriate.
- Determine whether outside legal counsel should be procured.

D. Implement remediation measures:

- Review access controls and procedures, including those in place before the Data Security Incident and those implemented during containment efforts, and address all know weaknesses.
- Assess operations to determine whether any revisions are necessary to data collection, retention, processing, or storage policies.
- Assess whether additional employee training is necessary or appropriate, and develop and implement training programs.
- Review and update privacy notices and commitments as necessary.
- Review compliance with this plan and determine whether any revisions or further training is necessary or appropriate.
- Consider whether disciplinary action against any employee is necessary or appropriate.
- Conduct final "after action" review and debriefing regarding overall incident and "lessons learned."

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