Definitions

Security incident: Refers to an adverse event in an information system, and/or network, or the threat of the occurrence of such an event. Incidents can include, but are not limited to, unauthorized access, malicious code, network probes, and denial of service attacks.

Overview

Security Incident Management at {COMPANY-NAME} is necessary to detect security incidents, determine the magnitude of the threat presented by these incidents, respond to these incidents, and if required, notify {COMPANY-NAME} members of the breach.

Purpose

This policy defines the requirement for reporting and responding to incidents related to {COMPANY-NAME} information systems and operations. Incident response provides {COMPANY-NAME} with the capability to identify when a security incident occurs. If monitoring were not in place, the magnitude of harm associated with the incident would be significantly greater than if the incident were noted and corrected.

This policy applies to all information systems and information system components of {COMPANY-NAME}. Specifically, it includes:

- Mainframes, servers, and other devices that provide centralized computing capabilities.
- Devices that provide centralized storage capabilities.
- Desktops, laptops, and other devices that provide distributed computing capabilities.
- Routers, switches, and other devices that provide network capabilities.
- Firewalls, Intrusion Detection/Prevention (IDP) sensors, and other devices that provide dedicated security capabilities.

In the event a breach of member's information occurs, {COMPANY-NAME} is required by Wisconsin state law to notify the individual(s) as described in Wisconsin Statute Section 895.507(2).

Policy Detail

Program Organization

- **Computer Emergency Response Plans** - {COMPANY-NAME} management must prepare, periodically update, and regularly test emergency response plans that provide for the continued operation of critical computer and communication systems in the event of an interruption or degradation of service. For example, Charter connectivity is interrupted or an isolated malware discovery.
- **Incident Response Plan Contents** - The {COMPANY-NAME} incident response plan must include roles, responsibilities, and communication strategies in the event of a compromise, including notification of relevant external partners. Specific areas covered in the plan include:
    - Specific incident response procedures
    - Business recovery and continuity procedures
    - Data backup processes
    - Analysis of legal requirements for reporting compromises
    - Identification and coverage for all critical system components
    - Reference or inclusion of incident response procedures from relevant external partners, e.g., payment card issuers, suppliers
- **Incident Response Testing** - at least once every year, the IT Department must utilize simulated incidents to mobilize and test the adequacy of response. Where appropriate, tests will be integrated with testing of related plans (Business Continuity Plan, Disaster Recovery Plan, etc.) where such plans exist. The results of these tests will be documented and shared with key stakeholders.

- **Incident Response and Recovery** - A security incident response capability will be developed and implemented for all information systems that house or access {COMPANY-NAME} controlled information. The incident response capability will include a defined plan and will address the seven stages of incident response:
    - Preparation
    - Detection
    - Analysis
    - Containment
    - Eradication
    - Recovery
    - Post-Incident Activity
  - To facilitate incident response operations, responsibility for incident handling operations will be assigned to an incident response team. If an incident occurs, the members of this team will be charged with executing the incident response plan. To ensure that the team is fully prepared for its responsibilities, all team members will be trained in incident response operations on an annual basis.
  - Incident response plans will be reviewed and, where applicable, revised on an annual basis. The reviews will be based upon the documented results of previously conducted tests or live executions of the incident response plan. Upon completion of plan revision, updated plans will be distributed to key stakeholders.

- **Intrusion Response Procedures** - The IT Department must document and periodically revise the Incident Response Plan with intrusion response procedures. These procedures must include the sequence of actions that staff must take in response to a suspected information system intrusion, who has the authority to perform what responses, and what resources are available to assist with responses. All staff expected to follow these procedures must be periodically trained in and otherwise acquainted with these procedures.
- **Malicious Code Remediation** - Steps followed will vary based on scope and severity of a malicious code incident as determined by Information Security Management. They may include but are not limited to: malware removal with one or more tools, data quarantine, permanent data deletion, hard drive wiping, or hard drive/media destruction.
- **Data Breach Management** - {COMPANY-NAME} management should prepare, test, and annually update the Incident Response Plan that addresses policies and procedures for responding in the event of a breach of sensitive customer data.
- **Incident Response Plan Evolution** - The Incident Response Plan must be updated to reflect the lessons learned from actual incidents. The Incident Response Plan must be updated to reflect developments in the industry.

Program Communication

- **Reporting to Third Parties** - Unless required by law or regulation to report information security violations to external authorities, senior management, in conjunction with legal representatives, the Security Officer, and the VP of IT must weigh the pros and cons of external disclosure before reporting these violations.
    - If a verifiable information systems security problem, or a suspected but likely information security problem, has caused third party private or confidential information to be exposed to unauthorized persons, these third parties must be immediately informed about the situation.
    - If sensitive information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, both its Owner and the Security Officer must be notified immediately.
- **Display of Incident Reporting Contact Information** - {COMPANY-NAME} contact information and procedures for reporting information security incidents must be prominently displayed in public communication mediums such as bulletin boards, break rooms, newsletters, and the intranet.
- Member Notification - The notification will be conducted and overseen by {COMPANY-NAME}'s Director of Risk Management. The notification should contain, at a minimum, the following elements:
    - Recommendations for the member to protect him/herself
    - Contact information for the Federal Trade Commission
    - Contact information for the credit bureaus

Sample notification letter:

[enter date here]

Dear [enter member's name here],

We, at {COMPANY-NAME} LLC, believe in acting quickly in our member's best interest. We recently became aware of an incident involving unauthorized access to certain member's confidential information. [describe here the incident in general terms]

We have taken steps to mitigate the incident and protect our member's information

from further risk. [describe here the steps taken by {COMPANY-NAME} in general terms]

This incident may have increased the probability of your information being used for fraudulent purposes. It is impossible to know with certainty whether you will experience trouble, but there are steps you can take to protect yourself. Here are some recommendations:

- Carefully review your account statements. If anything looks suspicious, promptly report the suspicious activity to {COMPANY-NAME}.
- Visit the Federal Trade Commission's (FTC) web site or call their toll-free number to obtain identity theft guidance and to report suspected incidents of identity theft.
    - http://www.ftc.gov/bcp/edu/microsites/idtheft//
    - Phone: 1-877-438-4338
    - TTY: 1-866-653-4261

- The Fair Credit Reporting Act allows you, under certain circumstances, to place a fraud alert in your consumer credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a victim of fraud. Placing a fraud alert in your file entitles you to order one free copy of your credit report from each agency. Review your credit reports carefully for unauthorized inquiries or accounts you did not open.

- TransUnion:
  Fraud Victim Assistance Division PO Box 6790
  Fullerton, CA 92834-6790
  1-800-680-7289
  www.transunion.com

- Equifax:
  PO Box 740241
  Atlanta, GA 30374-0241
  1-800-525-6285
  www.equifax.com

- Experian:
  PO Box 9554
  Allen, TX 75013
  1-888-397-3742
  www.experian.com

- You will need to remain observant for the next 12 to 24 months in checking your accounts for suspicious activity. Promptly report incidents of suspected identity theft to {COMPANY-NAME}.
- It is recommended that you obtain credit reports periodically from each of the nationwide credit reporting agencies and have information relating to fraudulent transactions deleted. Subscription services are available that can provide notification to you anytime there are changes or inquiries in your credit record.

Please do not hesitate to contact {COMPANY-NAME} LLC at 608-755-6065 or 800-779-5555 for assistance and information related to this incident.

Sincerely,

{COMPANY-NAME} LLC