Privacy and Data Security Incident Response Plan
Version 1.1
Updated January 2022

Contact: John Hanley, President Owner	260-267-9652
Alternate: Lindy Fritz, General Manager	260-200-6515

What is a Security Incident?

A security incident may involve any or all of the following:

- A violation of Company computer security policies and standards,
- unauthorized computer access,
- loss of information confidentiality,
- loss of information availability,
- compromise of information integrity,
- a denial-of-service condition against data, network or computer,
- misuse of service, systems or information, or
- physical or logical damage to systems or information.

Security incident examples include the presence of a malicious application, such as a virus; establishment of an unauthorized account for a computer or application; unauthorized network activity; presence of unexpected/unusual programs; or computer theft.

Incident Reporting

All suspected or confirmed privacy or data security incidents must be reported in accordance with Company policy. Workforce members that identify a potential incident will initially classify the incident severity based on their perception. The initial severity level may be escalated or de-escalated by the Information Technology staff for an electronic incident. All incident reports are to be made as soon as possible after the incident is identified, and with minimum delay for medium to high severity incidents.

Initial Incident Reports

Workforce member incident reports must include the following incident descriptors when describing the incident to their designated reporting point:

- date and time of incident discovery
- general description of the incident
- systems and/or data at possible risk
- actions they have taken since incident discovery
- their contact information

Containment Strategy

A containment strategy must be implemented that will limit the damage to Company resources. The containment strategy must include contact information for various Company organizations and personnel who may be involved in incident response. Containment may involve a

combination of technical controls, such as network and system disconnects, as well as media and communications to the public and to staff, depending upon the scope of the breach.

Identify and Engage Relevant Expertise

Identifying and engaging groups and individuals with relevant expertise are critical to accurately triage an incident and determine its scope. In large or complex cases, the Company will bring in a third party, such as an external organization, to assist in the triage and scoping effort. In order to verify insurance coverage, the insurance carrier may conduct a forensic investigation and participate in the incident response activities. Cooperation with the insurance carrier is required under the terms and conditions of the insurance policy.

External organization to contact:
4EOS
9815 Dawsons Creek Blvd
Fort Wayne, IN 46825
Phone: 260-490-7740

Technical Action

Specific technical review activities should include:

- Review whether remediation of affected local system(s) is complete.
    - Vulnerable hardware or software has been hardened against any break-ins, future attacks, or other security issues (e.g., installed patches, updated versions, replaced vulnerable sections of code).
- Conduct a root-cause analysis
- Assess whether security vulnerabilities can be adequately remediated by making changes within the current environment or a new/replacement environment should be created.
- Take needed actions to restore essential systems to functioning status, either in the original or a repaired environment, or determine that the activities must cease or be suspended until a different or rebuilt environment can be created. If replacing the environment:
    - Review technology choices
    - Design proposed new environment
    - Create new (replacement) environment
    - Bring in preserved data or re-create the data anew
- Identify any areas where different technical measures would have prevented the breach or improved results in this environment. Also identify what technical measures worked well.
- Consider whether continuous monitoring of the local environment needs to be implemented or enhanced, including what type(s), and whether an outside neutral party should conduct the monitoring.
- Analyze whether to recommend additional types of reviews in the local environment or elsewhere throughout the Company.
- Share lessons learned with appropriate contacts.

Communication/Disclosure Strategy

Proper handling of internal and external communications is critical in the initial phases of incident response. It is quite possible that an initially small incident could blossom into a larger incident or that a suspected incident could be determined to be unfounded. Improper handling of communications could lead to embarrassment to the Company in the event of a false positive, or could tip off any malicious attackers to cover their tracks, thus exposing the Company to more risk.

Legal counsel should be consulted to determine whether the investigation will proceed under the direction of counsel and attorney-client privilege. If so, counsel may establish particular procedures for communication and documentation.

Timing of Notifications

Customers will be notified within 60 days of the discovery of a data security breach incident which could have resulted in unauthorized access to a customer's confidential materials or that poses a threat to the security and confidentiality of such materials. The Company, as a Business Associate, will follow HIPAA and HITECH guidelines for regulatory requirements including individual notice and media notice.

1140 Hayden Street, Ste A
Fort Wayne, IN 46803
office: (260) 267-9652
fax: (260) 203-4489
info@federal-recordsmanagement.com
www.Federal-RecordsManagement.com