Polk County Wisconsin

ADMINISTRATIVE SAFEGUARDS

Security Incident Policy and Procedures

45 CFR §164.308 (a)(6)(i)

Required Standard

Policy 602.M

Effective Date: October 12, 2004 Revised Date:

Policy

A. Polk County Government will implement policies and procedures in compliance with the Security Rule to identify and respond to suspected or known security incidents; mitigate to the extent practicable, harmful effects of security incidents that are known to Polk County Government; and document security incidents and their outcomes.

B. Security incident means an attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with operations in an information system.

C. Polk County Government will:

1. Identify suspected or known security incidents.
2. Respond to suspected or known security incidents.
3. Mitigate to the extent practicable any harmful effect of security incidents that are known to Polk County Government.
4. Document security incidents and their outcomes.

D. The Information Technology Department will develop, implement and monitor policies and procedures to address security incidents.

Procedures

A. The Information Technology Department will develop, implement and monitor policies and procedures to address security incidents.

B. The Information Technology Department will supervise identification and reporting of security incidents. See *Response and Reporting Policy and Procedures.*

C. The Information Technology Department will be responsible for training all workforce members and other users in relation to identification, response and reporting of security incidents. See *Security Awareness and Training Policy and Procedures and Response* and *Reporting Policies and Procedures.*

D. The Information Technology Department will be responsible for investigation of a security incident. See *Investigation of Security Incident Policy and Procedures.*

E. The Information Technology Department will respond to all security incidents. See *Response and Reporting Policy and Procedures.*

F. The Information Technology Department will be responsible for mitigation of security incidents. See *Response and Reporting Policy and Procedures.*

G. The Information Technology Department will be responsible for documentation and retention of all materials related to security incidents for at least six years from the date of creation. See *Investigation of Security Incident Policy and Procedures, Response* and *Reporting Policies and Procedures, Security Incident Log* and other appropriate forms.

H. The Information Technology Department will be responsible for all enforcement activities related to a security incident. See *Security Incident Enforcement Policy and Procedures.*