

Polk County Wisconsin
ADMINISTRATIVE SAFEGUARDS
Security Management Process
Information System Activity Review Policy and Procedures
§164.308 (a)(1)(ii)(D)
Required

Policy 602.G

Effective Date: October 12, 2004

Revised Date:

Policy

- A. Polk County Government will implement procedures to ensure regular review of records of information system activity. Review of records may include audit logs, access reports and security incident tracking reports.
- B. Polk County Government will ensure through regular review of records of information system activity that security risk is appropriately monitored and reviewed.
- C. The Information Technology Department will be responsible for development and implementation of procedures to ensure annual review of records of information system activity.
- D. The Information Technology Department will be responsible for monitoring, reviewing and responding to the review of information system activity.

Procedures

- A. The Information Technology Department will develop and implement an internal audit procedure that will provide regular review of records of information system activity.
 - 1. The internal audit procedure may utilize audit logs, activity reports or other mechanisms to document and manage information system activity.
 - 2. The procedures implemented to provide review will be designed to promote a annual review of information system activity that will assist in the identification of potential and/or actual security breaches so that immediate corrective action may be taken.
- B. The internal audit procedure reviewing information system activity will be performed by the Information Technology Department.

C. The internal audit procedure will include:

1. Identification of electronic data sites;
2. Identification of information to be collected from the data sites that will assist in identification of actual and/or potential security issues;
3. Assimilation of information from the data collection sites into a report format that will be useful for reviewing electronic information system activity and assist in identification of security issues; and
4. Annual, or as deemed necessary, review of designated records or reports of information system activity. See *Information System Activity Review Form*.

D. The Information Technology Department will develop, implement and monitor all necessary information system review reports.

1. The Information Technology Department will identify what information or reports are needed by the information system to adequately audit internal electronic security processes.
2. The Information Technology Department will develop all reports necessary to adequately monitor the electronic information system(s).
3. The Information Technology Department will annually, or as deemed necessary, review the electronic system activity reports.
4. The Information Technology Department, based on review of information system activity reports, will develop parameters for “normal” or ”average” activity levels. Normals may be based on access at a specific site, frequency of access or other relevant criteria.

E. Based on development of “normal” information system levels, the Information Technology Department will be responsible for investigating identified abnormalities or unusual information system activities. Investigation may include:

1. Interview of workforce member(s);
2. Review of information system activity; and/or

F. The Information Technology Department will be responsible for any necessary response to the identified security abnormality. The response may include:

1. Correction of any information system security problem.
2. Workforce member education or sanction. See *Security Awareness and Training Policy and Procedures* and *Policy 601.P Confidentiality, Security and Access to PHI and Policy 716 Employee Discipline*.

- G. The Information Technology Department will be responsible for collecting, documenting and maintaining information system activity reports and related activities, including investigation and mitigation.
- H. Documentation of information system activity review, investigation and/or resolution will be maintained by the Information Technology Department for a minimum of six years from the date the information was created.