

Network Protection for Design Professionals

Logging, Monitoring and Auditing

Background:

Logging, monitoring and auditing — are used to track system activity both by system and application processes and by user activity on those systems and applications. These controls are designed to prevent the loss of confidentiality, integrity, or availability of information, including data and software, wherever stored within the organization's information systems. Processes such as these, provide the individual accountability, event reconstruction capability and means of intrusion detection which are needed to protect Non-Public Personal Information from unauthorized access. Likewise the "chain of custody" documentation of access to information is necessary to provide accountability for information stored on all types of media.

How to implement appropriate controls:

In regards to Non-public Personal Information entrusted to your organization, implement processes and tools which track and record the identity of those who access or have custody of this information; and record the time at which the access or custody takes place.

These procedures should include:

- Logging all attempted access to sensitive data.
- Logging successful authentication to applications or databases housing sensitive data, along with as much detail of subsequent activity as possible (files accessed, deleting records or fields, printing reports, etc.).
- Maintaining these logs in a tamper evident file and limiting access to these files for separation of duties.
- Reviewing logs daily for suspicious activity.

Resources:

An Introduction to Computer Security: The NIST Handbook Chapters 14 and 18, National Institute of Standards and Technology,

<http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf>

Common Sense Guide to Prevention and Detection of Insider Threats, United States Computer Emergency Readiness Team,

http://www.us-cert.gov/reading_room/

