

# IT Audit Information

2008 Tennessee Digital Summit



## Objectives

- ✓ Backups
- ✓ Disaster Recovery Planning
- ✓ Data Files
- ✓ Hardware Disposals
- ✓ Data Confidentiality
- ✓ Computer Forensics



## Backups

- Daily, Weekly & Yearly
- Configured Correctly
- Testing
- Off-site



## Disaster Recovery Planning

- Communication
- Provide help
- Keep it current
- Testing



## Data Files

- Get files for auditors
- Work with vendors to provide the needed format
- Help identify files that may be helpful
- Current file layouts that we want



## Hardware Disposals

- What not to do
- Document procedures
- Test your procedures
- Communicate policies



## Confidential Data

- ◆ Do I have confidential data?
- ◆ What do I do if this data is compromised?



## The Process

- ◆ Take an inventory of your data.
- ◆ Classify it into categories of sensitivity.
- ◆ Perform a risk assessment.
- ◆ Determine ways to protect the data.
- ◆ Perform a cost/benefit analysis.
- ◆ Develop and implement your policies.



## Do I have confidential data?

- ◆ [Section 47-18-2107, Tennessee Code Annotated](#)
  - Defines "personal information" as a first and last name in combination with any of the following:
    - ◆ Social security number
    - ◆ Driver license number
    - ◆ Acct # in combination with required access code



## What do I do if this data is compromised?

- ◆ [Section 47-18-2107, Tennessee Code Annotated](#)
  - Requires notification to any resident when his/her personal information may have been compromised.



## Computer Forensics

- Computer User Agreements
- Contact the auditors
- Use appropriate tools
- Real life examples



## Questions?



## Contact Information

---

**Nathan Abbott – [nathan.abbott@state.tn.us](mailto:nathan.abbott@state.tn.us)**

**615-401-7841**

