SOUTH CAROLINA TRUSTWORTHY INFORMATION SYSTEMS HANDBOOK

TABLE OF CONTENTS

Appendices

A1 Glossary
Defines terms that are used throughout the *Handbook*

A2 Bibliography
Provides citations to works consulted during *Handbook* development

A3 Citation
Citation of the *Trustworthy Information Systems Handbook*

A4 Background Information
Background of the Trustworthy Information Systems Project

A5 Methodology
Trustworthy Information Systems Project Methodology

A6 South Carolina Laws and Policies
South Carolina Laws and Policies Relating to Electronic Records

A7 Legal Issues
Legal Issues Affecting Electronic Records Management

PART 1: Introduction[1]

1.1: Why is a trustworthy information system important?

Records and information in government are extremely important for the following reasons:

- They facilitate government business
- They demonstrate government accountability
- They serve as evidence of government activity in South Carolina for current and future users of government information

In the face of the rapid growth of information technology, government information systems must demonstrate accountability through sound information management and documentation of government activity. Increasingly, attorneys are making electronic evidence a central focus of litigation. Courts, too, are paying attention and recognizing that electronic data means more than obtaining a printout of computer files. For instance, the Federal Code of Civil Procedure requires litigants to disclose categories and locations of relevant electronic files early in the litigation process or risk the possibility of an on-site search of their computer system. As a result of our evolving legal environment, you are required to maintain accurate electronic files and any destruction of data must be scheduled and carried out in a timely manner. Failure to properly plan or care for electronic data and records could make it harder to find and produce legally admissible records when required by law.

You can lessen the likelihood for problems through practical measures. At a minimum, you should know what information your system holds and how you can find it quickly and cost effectively. Additionally, you must also take steps to prove to the court that you have established and strictly followed well-documented procedures that prevent unauthorized access to your files and that the systems you manage provide timely and accurate information.

Producing trustworthy information is an attainable goal that should be an objective of every system manager. The following handbook is designed to assist you in creating and maintaining trustworthy information systems. We have developed this handbook to encourage you to practice good records management within an automated environment. They can help you, as a state or local government agency manager, produce records that meet everybody's needs — yours, the court's, the auditor's, and any other legitimate record user's. This handbook can be used for evaluating the trustworthiness of any government information system — large or small, old or new. It provides a valuable set of proven tools that your agency can apply, practically and efficiently. We encourage you to make this handbook your own!

---

[1] This handbook is adapted from the *Trustworthy Information Systems Handbook*, Version 4, July 2002, written and published by the Minnesota State Archives [www.mnhs.org/preserve/records/tis/tis.html]. It also references the international standard *ISO 15489-2*, First Edition, 2001-09-15.

1.2: What is a trustworthy information system?

Trustworthiness refers to an information system's accountability and its ability to produce reliable and authentic information and records.

We use the words authenticity, reliability and integrity when we talk about the information and records that the information system creates. Understanding these concepts is key to developing a trustworthy information system.

Authenticity
Authenticity simply means a record is what it purports to be. An authentic record is one that can be proven.

a) to be what it purports to be,
b) to have been created or sent by the person purported to have created it or sent it, and
c) to have been created or sent at the time purported

Reliability
Reliability refers to the authority and trustworthiness of records as evidence — their ability to stand for the facts.

a) A reliable record is one whose contents can be trusted as a full and accurate representation of the transactions, activities or facts to which they attest and can be depended upon in the course of subsequent transactions or activities.

Unfortunately, a record can be authentic but not reliable. An authentic record will not be considered reliable when, over time, some part of its content, structure or context has been lost.

Integrity
The integrity of a record refers to its being complete and unaltered. If your records management policy allows for changes to a record after it is created, strict control of this process must be maintained. This includes specifying who is allowed to make any additions, deletions or annotations and under what circumstances. Any authorized annotation, addition or deletion to a record should be explicitly indicated and traceable.

With electronic records and information in digital formats, we cannot demonstrate reliability, authenticity and integrity as easily as we can with paper records. We cannot see, touch, or examine electronic records in any intelligible way without the assistance of hardware and software. The computer, unlike a human being, does not bear accountability for itself; people in government make information systems accountable. It follows, then, that in building information systems, we need to establish and create procedures, system documentation, and descriptions of system information as a means to make the system accountable. This handbook provides the next best thing — the tools needed to examine government information systems for trustworthiness

1.3: What is the process for establishing trustworthiness?

Establishing the trustworthiness of an information system typically takes several steps and requires the collaboration of people with a variety of skills and knowledge. The Handbook's structure parallels the process and guides the reader along. Part 1, which you are reading now, provides background to help you get started. Parts 2 and 3 contain the criteria sets and checklists to help you evaluate your systems. Those undertaking the examination process for the first time are strongly encouraged to read through the entire handbook completely before beginning their project. Each successive step in the process builds on those before and it is important that none be slighted or skipped. The proper establishment of the trustworthiness of an information system depends on the completeness of the examination process.

Step 1: Assemble team ***(Section 1.4: "Who should participate?")***

Step 2: Choose a criteria selection method ***(Section 1.5 "How do you apply the trustworthy information systems criteria" & 1.6: "When can you apply the trustworthy information systems criteria?)***

Step 3: Determine the importance of the information in the system ***(Section 1.7: "How important is your information?")***

Step 4: Document the process ***(Section 1.8: "Why are metadata and documentation important?")***

Step 5: Select appropriate criteria ***(Section 2.1: "What are the criteria for a trustworthy information system?")***

Step 6: Implement and document choices ***(Section 1.8: "Why are metadata and documentation important?")***

1.4: Who should participate?

The *Handbook* encourages collaboration among a variety of people with diverse sets of skills and expertise. They are valuable assets in reaching your goal of information system trustworthiness.

Ideally, teams of agency personnel with a range of skills and knowledge will work together in this process. Your team should include people who have:

- Knowledge of agency and local government business, policy, and procedures. They know which laws and policies apply to your agency's information. Agency attorneys and auditors are valuable in this area.
- Knowledge of information access and data practices. They know who can access the information and for what reasons, and how long information needs to remain accessible. Agency records managers and the South Carolina Department of Archives and History can help in the process.
- Skills in computing, information technology, and information systems design. They can provide advice and propose options on what technologies and methodologies would work to accomplish business needs. Your information systems and technology staff, and even selected vendors, should be able to provide answers to questions.

The team should first be educated and made aware of the importance of information system trustworthiness and why the evaluation process is necessary. The team also needs to know the value of documenting their decisions, and they should be kept appraised of progress while system development is underway.

With a diverse and knowledgeable team assembled, you are on the right track for establishing information system trustworthiness.

1.5: How do you apply the trustworthy information systems criteria?

The Trustworthy Information Systems (TIS) criteria can be used in many ways depending on your agency's particular situation. Use of the criteria varies depending on a number of agency-specific factors such as:

- Agency information needs and policies
- Information system size, type, and scope
- Phase of information system development life cycle
- Agency size, staff, and procedures

The TIS criteria set presents itself much like a cafeteria line, with a wide array of criteria choices in different categories. The costs for implementing any of the criteria vary. If you think about a cafeteria line, customers make choices based on their hunger, dietary needs, and budgets.

In the TIS criteria cafeteria line, agency information system development teams face similar choices:

- What criteria items do we absolutely need to do our business and to meet information requirements?
- Which ones would be nice to have?
- What are the costs of implementing selected criteria?
- What are the costs (up-front and hidden) associated with not implementing them?

Agencies have different information needs and operate under different policy mandates and statutes. What's important to one agency may have little relevance to another. Therefore, the choices you make should represent what is appropriate for your organization and the individual information system(s).

1.6: When can you apply the trustworthy information systems criteria?

You can use the *Handbook* at any time during information system development. It is never too late to think about system trustworthiness. However, the earlier during the system development life cycle that you consider its trustworthiness, the better off you'll be.

Option 1: Applying the handbook during system design and development

During the analysis phase of system development, before a lot of time and money is spent on system design, is the most opportune time to weigh all of the TIS criteria that might be important to implement. At this time, you can think about the big picture without the constraints of a system that's already well along in development or operation. The steps in this instance are as follows:

1) Determine the value of your data
2) Weigh that value against the costs (time, money, etc.) of implementing each criteria
3) Choose only those criteria that support your determined level of risk
4) Implement
5) Document your choices (including handbook version, refer to Appendix A) and actions
6) Reassess needs and risks on a regular basis

Option 2: Applying the handbook to an existing information system

Obviously, establishing the trustworthiness of an information system is a process most easily undertaken during the analysis/planning phase before the design is nailed down. That's the ideal, but most agencies don't have that luxury. The handbook is useful at any point during the system development life cycle and can be used to examine the trustworthiness of systems that are already in place — your legacy systems. You can document what you presently have and establish how well the system is set up to meet various requirements. The steps in this instance are as follows:

1) Determine the value of your data
2) Examine your system with reference to the criteria
3) Determine which are already in place
4) Ask whether your current system configuration offsets your risks
5) Choose additional criteria for implementation after weighing the costs
6) Implement
7) Document your choices (including handbook version) and actions
8) Reassess needs and risks on a regular basis

Information systems are not static; they must respond to changes all the time. Changes in software, hardware, platforms, means of communications, and growth occur rapidly and necessitate considering and revisiting the TIS criteria on a periodic basis. Documentation of what you presently have can serve as a check on how well the system is set up to meet your various requirements.

1.7: How important is your information?

Determining Value/Assessing Risk

Records and data are not all equally valuable. Therefore, not all information systems containing records will require the same security measures and levels of trustworthiness. In determining the value of your information, you may want to consider such things as:

- What records and data are essential to your performing your business functions?
- What data is of permanent and/or historical value to you and to others?

In addition to determining value, you should also explore the risks associated with your information system. Again, not all information systems are equal. Losing data in some systems presents little more than an inconvenience. "At-risk" systems have a greater potential for legal problems and are financial liabilities. In many ways, this handbook serves as a risk management tool to limit your liability, both financial and legal. Questions you may ask include:

- What laws and regulations apply to your data?
- What areas and records might lawyers and auditors target?
- What are your industry's standards for system security, data security, and records retention?

Use the risk worksheet to evaluate the value and risk associated with your records.

1.8: Why are metadata and documentation important?

Documentation and metadata serve as the fundamental foundation of any trustworthy information system, enabling proper data creation, storage, retrieval, use, modification, retention, and destruction.

Documentation has two meanings. On a broad level, it is the process of recording actions and decisions. On a system level, documentation is information about planning, development, specifications, implementation, modification, and maintenance of system components (hardware, software, networks, etc.). System documentation includes such things as policies, procedures, data models, user manuals, and program codes. Documentation capture is not a system process.

Metadata can be simply defined as "data about data." More specifically, metadata consists of a standardized structured format and controlled vocabulary which allows for the precise description of record content, location, and value. Metadata often includes items like file type, file name, creator name, date of creation. Metadata capture, whether automatic or manual, is a process built into the actual information system.

Documentation and metadata establish accountability for information systems, and accountability goes hand-in-hand with trustworthiness — the ability to produce reliable and authentic records.

From the very beginning of your examination process, no matter where in the information system development life cycle you start, you must make a conscious effort to keep documentation. Documentation gathered after the fact always carries the possibility of incorrectness and/or incompleteness. Begin by gathering such information as:

- System name, owner, life cycle phase, purpose, etc.
- Rationale for the examination process
- Names and functions of team members
- Dates

As the examination process moves along, collect other documentation as appropriate. For example:

- Which version of the *Handbook* was used?
- Which criteria were selected? Why?
- Which criteria were not selected? Why?
- What were the responses to the various additional considerations?
- Who is responsible for implementation of the chosen criteria and each piece of supporting documentation?
- When were your choices implemented?

At the end of your initial system examination, you should have a complete record of your process and the choices you made along the way. By following up with consistent application of your choices and by maintaining the currency of your documentation as you make changes and revisit the criteria set, you will not only have an effective management tool for your system's proper administration, you will have evidence of its trustworthiness.

Bear in mind: complete documentation of an entire system is a daunting task that may not always be necessary for your particular situation — perhaps only certain functions need the careful attention outlined above. The value of your records must be weighed against cost and risk. Use the chart on the next page to gauge the various risks associated with your records before starting Part 2.

WHAT RISKS DO YOUR RECORDS AND RECORDS KEEPING PRACTICES POSE FOR YOU?

Do you have a records management program in place?

Approved, detailed current retention schedules ⟷ No program

Do you document your record keeping systems and practices?

Current data models, data dictionaries, procedures ⟷ No documentation

Do your records have a high audit and/or legal value?

Never audited or sued ⟷ Routinely audited and subject to litigation

Do you have a plan to preserve your vital records in case of disaster?

Current, comprehensive plan ⟷ No plan

Do your records contain confidential and private data?

No — only public data ⟷ Yes — there are significant data practices and privacy concerns

Do citizens and journalists request access to your records?

Never ⟷ Routinely

Do your records have historic value?

No historic value ⟷ Significant value to historians and genealogists

Do you have system security procedures in place?

Fully documented trustworthy system ⟷ No correlation of security needs with statutory mandates

PART 2: Criteria for Trustworthy Information Systems

The following criteria outline the best available practices for implementing a trustworthy information system. The most appropriate practices for a particular system may comprise only a certain number of these. Agencies choose what is reasonable and practical depending on a variety of factors. The important point is to make, justify, and document your choices in order to ensure consistent application and your agency's accountability for its decisions.

QUESTIONS TO ASK

What laws and/or regulations (state and federal) apply to the data within your system?

What are your industry's standards for system security?

What are your industry's standards for data security?

What areas/records might lawyers target?

What areas/records might auditors target?

What data is of permanent/ historical value to you and/or to others?

The criteria range from system- to record-level and are categorized into five main groups:

- system documentation
- security measures
- audit trails
- disaster recovery plans
- record metadata

Each of these areas contain specific criteria as well as items for further consideration:

- *Did You Know* highlights items drawn from South Carolina government sources concerning information systems and records management.
- Points under *Consider This* expand upon the criteria.
- The left-hand sidebar offers general *Questions to Ask* while working with the criteria set; those opposite a particular criteria group are complementary to its issues.

The criteria set will be updated as necessary to reflect new information. Sources are listed in the Bibliography section of this handbook.

Criteria Group 1: *System administrators should maintain complete and current documentation of the entire system.*

1A. System documentation should include, but is not limited to:

1. hardware (procurement, installation, modifications, and maintenance)
2. software (procurement, installation, modifications, and maintenance)
3. communication networks (procurement, installation, modifications, and maintenance)

Did You Know:

▲". . . all governmental bodies, as defined in the procurement code, must develop, in coordination with the CIO, a master plan for information technology procurements. Subject to CIO approval of the master plan, acquisitions of information technology by governmental bodies shall be through the CIO's Information Technology Management Office." (South Carolina CIO website.) www.cio.sc.gov/cioContent.asp?pageID=205

4. interconnected systems
   a. list of interconnected systems (including the Internet)
   b. names of systems and unique identifiers
   c. owners
   d. names and titles of authorizing personnel
   e. dates of authorization
   f. types of interconnection
   g. indication of system of record
   h. sensitivity levels
   i. security mechanisms, security concerns, and personnel rules of behavior

Consider This:

▲System documentation, including specifications, program manuals, and user guides, should be covered in retention schedules, and retained for the longest retention time applicable to the records produced in accordance with the documents.

▲Unique names and identifiers should remain the same over the lifetime of the units to allow tracking.

▲When a system is installed at more than one site, steps should be taken to ensure that each site is running an appropriate, documented, up-to-date version of the authorized configuration.

QUESTIONS TO ASK

What is the agency and department responsible for the system?

What is the agency and department responsible for applications?

What is the name and contact information of the person(s) responsible for system administration?

What is the name and contact information of the person(s) responsible for system security?

Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?

What is the system's unique identifier and/or common name?

If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?

Were design reviews and system tests run prior to placing the system in production? Were the tests documented?

▲ Audit trails of hardware and software changes should be maintained such that earlier versions of the system can be reproduced on demand.

▲ A process should be implemented to ensure that no individual can make changes to the system without proper review and authorization.

1B. Policy and procedure documentation should include, but is not limited to:

1. programming conventions and procedures
2. development and testing activities, including tools

Consider This:

▲ Periodic functional tests should include anomalous as well as routine conditions, and be documented such that they can be repeated by any knowledgeable programmer.

QUESTIONS TO ASK

Is application software properly licensed for the number of copies in use?

3. applications and associated procedures such as methods of entering/accessing data, data modification, data duplication, data deletion, indexing techniques, and outputs
4. identification of when records become official

Consider This:

▲ The South Carolina Department of Archives and History works with state agencies and local governments to ensure the proper management of South Carolina's public records, and to identify and protect those of historical value. We provide training and advisory services to state and local government offices and conduct training classes. For more information go to: www.state.sc.us/scdah/statelcl.htm

5. record formats and codes
6. routine performance of system backups. Each backup should be documented with backups being appropriately labeled, stored in a secure, off-line, off-site location, and subjected to periodic integrity tests.
7. routine performance of quality assurance and control checks, as well as performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers

Consider This:

▲ Identification devices (e.g., security cards) should be included in periodic testing runs to ensure proper functioning and to verify the correctness of identifying information and system privilege levels.

What other systems might records be migrated to?

▲ Each type of storage medium used should undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems.

8. migration of records to new systems and media as necessary. All record components should be managed as a unit throughout the transfer.
9. standard training for all users and personnel with access to equipment

Consider This:

▲ Users should sign statements agreeing to terms of use. Such a document should include guidelines for: user responsibilities and expected behavior, consequences of inconsistent behavior or non-compliance, remote access use, internet use, use of copyrighted works, unofficial use of resources, assignment and limitations of system privileges, and individual accountability.

Criteria Group 2: *System administrators should establish, document, and implement security measures.*

2A. User Identification / Authorization

QUESTIONS TO ASK

Is system performance monitoring used to analyze system performance logs in real time to look for availability problems, including active attacks, and system and network slowdowns and crashes?

1. User identification and access procedures should be established and documented. Users should be authenticated prior to being granted access.
2. Each user should be assigned a unique identifier and password. Identifiers and passwords should not be used more than once within a system. Use of access scripts with embedded passwords should be limited and controlled.

Consider This:

▲ Upon successful log-in, users should be notified of date and time of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry.

▲ Where identification codes in human-readable form are considered too great a security liability, other forms should be employed such as encoded security cards or biometric-based devices.

Is there a list of all internal and external user groups and the types of data created and/or accessed?

3. Password rules should include standard practices such as minimum password length, expiration dates, and a limited number of log-on attempts. System administrators should determine what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger the notification of security personnel.
4. Users should be restricted to only the level of access necessary to perform their job duties.

QUESTIONS TO ASK

What are the procedures for the destruction of controlled-access hard copies?

Who can invoke change mechanisms for object, process, and user security levels?

Who (creator, current owner, system administrator, etc.) can grant access permissions to a record after the record is created?

5. Permission to alter disposition/retention codes, and/or to create, modify, and delete records should be granted only to authorized users with proper clearance. Modification of record identifiers is not allowed.
6. Access to private keys for digital signatures should be limited to authorized individuals.
7. Lists of all current and past authorized users along with their privileges and responsibilities should be maintained. The current list should be reviewed on a regular schedule to ensure the timely removal of authorizations for former employees, and the adjustment of clearances for workers with new job duties.
8. Personnel duties and access restrictions should be arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions. No individual should have the ability to single-handedly compromise the system's security and operations.

2B. Internal System Security

1. Access to system documentation should be controlled and monitored.
2. Access to output and storage devices should be controlled and monitored.

Have all positions been reviewed with respect to appropriate security levels?

How is information purged from the system?

How is reuse of hardware, software, and storage media prevented?

3. Controls should be in place to ensure proper security levels of data when archiving, purging, or moving from system to system. Controls should be in place for the transportation or mailing of media or printed output.
4. Procedures should be implemented to ensure the complete sanitization and secure disposal of hardware, software, and storage media when outdated or supplanted by newer versions, units, etc. Documentation should include date, equipment identifiers, methods, and personnel names.
5. Insecurity-detection mechanisms should be constantly monitoring the system. Fail-safes and processes to minimize the failure of primary security measures should be in place at all times.
6. Security procedures and rules should be reviewed on a routine basis to maintain currency.

QUESTIONS TO ASK

Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?

7. Measures should be in place to guard the system's physical security. Items to consider include:
   a. access to rooms with terminals, servers, wiring, backup media
   b. data interception
   c. mobile/portable units such as laptops
   d. structural integrity of building
   e. fire safety
   f. supporting services such as electricity, heat, air conditioning, water, sewage, etc.
8. Security administration personnel should undergo training to ensure full understanding of the security system's operation.

2C. External System Security

1. In cases of remote access to the system, especially through public telephone lines, additional security measures should be employed. Possible action could include the use of input device checks, caller identification checks (phone caller identification), callbacks, and security cards.
2. For records originating outside the system, the system should be capable of verifying their origin and integrity. At a minimum, the system should:
   a. verify the identity of the sender or source
   b. verify the integrity of, or detect errors in, the transmission or informational content of the record
   c. detect changes in the record since the time of its creation or the application of a digital signature
   d. detect any viruses or worms present

Criteria Group 3: *System administrators should establish audit trails that are maintained separately and independently from the operating system.*

QUESTIONS TO ASK

Who can access audit data? Alter? Delete? Add?

How can the audit logs be read? Who can do this?

What tools are available to output audit information? What are the formats? Who can do this?

3A. General characteristics of audit trails include:

1. Audit trail software and mechanisms should be subject to strict access controls and protected from unauthorized modification or circumvention.
2. Audit trails should be backed up onto removable media periodically to ensure minimal data loss in case of system failure.
3. System should automatically notify system administrators when audit storage media is nearing capacity and response should be documented. When the storage media containing the audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of data it holds.

Consider This:

▲ If audit trails are encoded to conserve space, the decode mechanism must always accompany the data.

3B. A system should be in place to track password usage and changes. Recorded events and information should include:

1. user identifier
2. successful and unsuccessful log-ins
3. use of password changing procedures
4. user ID lock-out record
5. date
6. time
7. physical location

3C. A system should be in place to log and track users and their online actions. Audit information might include:

1. details of log-in (date, time, physical location, etc.)
2. creation of files/records
3. accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level)
4. accessed device identifiers
5. software use
6. production of printed output
7. overriding of human-readable output markings (including overwrite of sensitivity label markings and turning off of labeling mechanisms) on printed output
8. output to storage devices

QUESTIONS TO ASK

How are audit logs protected?

3D. For each record, audit trails should log, at a minimum, the following information:

1. record identifier
2. user identifier
3. date
4. time
5. usage (e.g., creation, capture, retrieval, modification, deletion)

What mechanisms are available to designate which activities are audited? Who can do this?

Criteria Group 4: *System administrators should establish comprehensive disaster and security incident recovery plans.*

4A. Disaster and security incident recovery plans should be periodically reviewed for currency and tested for efficiency.

Did You Know:

▲"To protect the state's critical information technology infrastructure and associated data systems in the event of a major disaster, whether natural or otherwise, and to allow the services to the citizens of this State to continue in such an event, the Office of the State Chief Information Officer (CIO) should develop a Critical Information Technology Infrastructure Protection Plan devising policies and procedures to provide for the confidentiality, integrity, and availability of, and to allow for alternative and immediate on-line access to critical data and information systems including, but not limited to, health and human services, law enforcement, and related agency data necessary to provide critical information to citizens and ensure the protection of state employees as they carry out their disaster-related duties. All state agencies and political subdivisions of this State are directed to assist the Office of the State CIO in the collection of data required for this plan." (*South Carolina Code of Laws*. Protection of critical information technology infrastructure and data systems. 1-11-435. www.scstatehouse.org/code/t01c011.htm

4B. Security incident recovery plans.

1. Hazards include:
   a. hardware failure or malfunction
   b. software failure or malfunction
   c. network failure or malfunction
   d. human error
   e. unauthorized access and activity
2. Government agencies should contact the Office of the State CIO for assistance with incident-handling procedures and support.
3. Related resources include :
   a. CERT Coordination Center [www.cert.org]

4C. Disaster recovery plans.

1. Hazards include:
   a. fire and/or explosion
   b. water or flood
   c. wind or tornado
   d. lightning
   e. hurricane
   f. power outage
   g. insects
   h. rodents
   i. violence and/or terrorism
   j. human error
2. Government agencies should contact the South Carolina Emergency Management Division and review the "South Carolina Emergency Operations Plan"
   a. The South Carolina Emergency Management Division can assist with:
      1. risk assessments
      2. recovery strategy development
      3. plan development
      4. training
      5. plan test coordination
      6. plan maintenance
   b. Information regarding the South Carolina Emergency Management Division and its services is available at: [www.scemd.org]
3. Related resources include:
   a. South Carolina Department of Archives and History disaster preparedness and recovery guidelines available at: [www.state.sc.us/scdah/techlflt.htm]
   b. Federal Emergency Management Agency (FEMA) emergency response and recovery guidelines available at [www.fema.gov]

Criteria Group 5: *Each record and/or record series should have an associated set of metadata.*

QUESTIONS TO ASK

What are the components of a complete or final record of a transaction?

What are the minimum components necessary to provide evidence of a transaction? If you went to court, what would be the minimum information you would need?

Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of a transaction or any of its components?

What information is necessary to interpret the contents of a record?

During which agency business processes might you have to access a record?

Who are the external secondary users of your records?

What are the rules, laws, and regulations that restrict or open access to these records to external secondary users?

What are the procedures for reproducing records for use by secondary users? What are the reproduction formats?

Is there a mechanism to indicate sensitivity level on hardcopies? Who can enable/ disable this function?

What are your industry's standards for records retention?

5A. This Recordkeeping Metadata Standard (developed by the state of Minnesota) includes twenty elements. Each is listed below along with associated sub-elements and the obligation for implementation.

1. **Agent** (**mandatory)
   Definition: An agency or organizational unit responsible for some action on or usage of a record. An individual who performs some action on a record, or who uses a record in some way.
   - 1.1 Agent Type (mandatory)
   - 1.2 Jurisdiction (mandatory)
   - 1.3 Entity Name (mandatory)
   - 1.4 Entity ID (optional)
   - 1.5 Person ID (optional)
   - 1.6 Personal Name (optional)
   - 1.7 Organization Unit (optional)
   - 1.8 Position Title (optional)
   - 1.9 Contact Details (optional)
   - 1.10 E-mail (optional)
   - 1.11 Digital Signature (optional)

2. **Rights Management** (**mandatory)
   Definition: Legislation, policies, and caveats which govern or restrict access to or use of records.
   - 2.1 MGDPA Classification (mandatory)
   - 2.2 Other Access Condition (optional)
   - 2.3 Usage Condition (optional)
   - 2.4 Encryption Details (optional)

3. **Title** (**mandatory)
   Definition: The names given to the record.
   - 3.1 Official Title (mandatory)
   - 3.2 Alternative Title (optional)

4. **Subject** (**mandatory)
   Definition: The subject matter or topic of a record.
   - 4.1 First Subject Term (mandatory)
   - 4.2 Enhanced Subject Term (optional)

5. **Description** (optional)
   Definition: An account, in free text prose, of the content and/or purpose of the record.

6. **Language** (optional)
   Definition: The language of the content of the record.

QUESTIONS TO ASK

What is the records disposition plan?

Who is responsible for authorizing the disposition of records?

Who is responsible for changes to the records disposition plan?

How does the system accommodate integration of records from other systems?

Who can access record metadata? Alter? Delete? Add?

SPECIAL QUESTIONS FOR DATA WAREHOUSES

Do you gather extraction metadata?

Do you cleanse the data? Do you document the procedure? Do you gather cleansing metadata?

Do you transform the metadata? Do you document the procedure? Do you gather transformation metadata?

What metadata and/or documentation do you offer users?

Who can access metadata? Alter? Delete? Add?

What are the legal liabilities regarding data ownership and custodial responsibilities? Where do data custody responsibilities reside — with the source systems, the warehouse system, or both?

Are there records retention schedules and policies for warehouse data? Is retention of warehouse data coordinated with retention for data extracted from the source systems?

7. **Relation** (optional)
   Definition: A link between one record and another, or between various aggregations of records. A link between a record and another information resource.
   7.1 Related Item ID (mandatory)
   7.2 Relation Type (mandatory)
   7.3 Relation Description (optional)

8. **Coverage** (optional)
   Definition: The jurisdictional, spatial, and/or temporal characteristics of the content of the record.
   8.1 Coverage Type (mandatory)
   8.2 Coverage Name (optional)

9. **Function** (optional)
   Definition: The general or agency-specific business function(s) and activities which are documented by the record.

10. **Date** (**mandatory)
    Definition: The dates and times at which such fundamental recordkeeping actions as the record's or records series' creation and transaction occur.
    10.1 Date/Time Created (mandatory)
    10.2 Other Date/Time (optional)

11. **Type** (optional)
    Definition: The recognized form or genre a record takes, which governs its internal structure.

12. **Aggregation Level** (**mandatory)
    Definition: The level at which the record(s) is/are being described and controlled. The level of aggregation of the unit of description (i.e., record or record series).

13. **Format** (optional)
    Definition: The logical form (content medium and data format) and physical form (storage medium and extent) of the record.
    13.1 Content Medium (mandatory)
    13.2 Data Format (mandatory)
    13.3 Storage Medium (mandatory)
    13.4 Extent (optional)

14. **Record Identifier** (**mandatory)
    Definition: A unique code for the record.

15. **Management History** (**mandatory)
    Definition: The dates and descriptions of all records management actions performed on a record from its registration into a recordkeeping system until its disposal.
    15.1 Event Date/Time (mandatory)
    15.2 Event Type (mandatory)
    15.3 Event Description (mandatory)

16. **Use History** (optional)
    Definition: The dates and descriptions of both legal and illegal attempts to access and use a record, from the time of its registration into a recordkeeping system until its disposal.
    16.1 Use Date/Time (mandatory)
    16.2 Use Type (mandatory)
    16.3 Use Description (optional)

17. **Preservation History** (optional)
    Definition: The dates and descriptions of all actions performed on a record after its registration into a recordkeeping system which ensure that the record remains readable (renderable) and accessible for as long as it has value to the agency and to the community at large.
    17.1 Action Date/Time (mandatory)
    17.2 Action Type (mandatory)
    17.3 Action Description (mandatory)
    17.4 Next Action (optional)
    17.5 Next Action Due Date (optional)

18. **Location** (**mandatory)
    Definition: The current (physical or system) location of the record. Details about the location where the record usually resides.
    18.1 Current Location (mandatory)
    18.2 Home Location Details (mandatory)
    18.3 Home Storage Details (mandatory)
    18.4 Recordkeeping System (optional)

19. **Disposal** (**mandatory)
    Definition: Information about policies and conditions which pertain to or control the authorized disposal of records. Information about the current retention schedule and disposal actions to which the record is subject.
    19.1 Retention Schedule (mandatory)
    19.2 Retention Period (mandatory)
    19.3 Disposal Action (mandatory)
    19.4 Disposal Due Date (mandatory)

20. **Mandate** (optional)
    Definition: A source of recordkeeping requirements. For example, a piece of legislation, formal directive, policy, standard, guideline, set of procedures, or community expectation which (explicitly or implicitly) imposes a requirement to create, keep, dispose of, or control access to and use of a record.
    20.1 Mandate Type (mandatory)
    20.2 Refers To (mandatory)
    20.3 Mandate Name (mandatory)
    20.4 Mandate Reference (optional)
    20.5 Requirement (optional)

Consider This:

▲ Where records are not individually authenitcated, record series metadata may include the name or title of the individual responsible for validating or confirming the data within the record series, and for confirming that the particular series was produced in accordance with standard procedures.

PART 3:
Criteria Group Checklists

The following checklists are designed to help you gather information about the information system(s) in your organization. It is divided into five main criteria groups as follows: *System Documentation, System Security, Audit Trails, Disaster Planning and Recovery* and *Metadata*. These criteria groups are explained in detail in Part 2 of this manual. An introductory section, *Questions to Consider*, and a supplementary section on *Data Warehousing* are also included here.

Complete the criteria from beginning to end for total system evaluation or, depending on your agency's needs, select those criteria groups that require review. How you proceed is entirely up to you. You can use the *Top Level Criteria* below and/or the *Legal Risk Analysis Tool* to help you select the applicable criteria checklists.

Top Level Criteria The following criteria should be used to establish a trustworthy information system. If you are unsure or unable to answer Yes to any of the following questions, go to the Criteria Group listed and complete the detailed analysis.	**In Place? Yes/No**	**Notes**
1. System administrators should maintain complete and current documentation of the entire system. *If unsure, go to **Criteria Group 1** to do an analysis of your documentation procedures.*		
2. System administrators should establish, document, and implement security measures. *If unsure, go to **Criteria Group 2** to do an analysis of your security procedures.*		
3. System administrators should establish audit trails that are maintained separately and independently from the operating system. *If unsure, go to **Criteria Group 3** to do an analysis of your audit procedures.*		
4. System administrators should establish a comprehensive disaster recovery plan. *If unsure, go to **Criteria Group 4** to do an analysis of your disaster recovery procedures.*		
5. Each record should have an associated set of metadata. *If unsure, go to **Criteria Group 5** to do an analysis of your metadata procedures.*		

Questions to Consider	Response
What laws and/or regulations (state and federal) apply to the data within your system?	
What are your industry's standards for system security?	
What are your industry's standards for data security?	
What areas/records might lawyers target?	
What areas/records might auditors target?	
What data is of permanent/historical value to you? To others?	

Criteria Group 1: System Documentation System Documentation Questions	Response
What is the system's unique identifier and/or common name?	
What is the agency and department(s) responsible for the system?	
What is the agency and department(s) responsible for applications?	
What is the name and contact information of the person(s) responsible for system administration?	
What is the name and contact information of the person(s) responsible for system security?	
Has a formal risk assessment of the system been completed? Date? Performed by? Methodology? Findings?	
Were design reviews and system test run prior to placing the system in production? Were the tests documented?	
Is application software properly licensed for the number of copies in use?	
If connected to external systems lacking commensurate security measures, what mitigation procedures are in place?	
What other systems might records be migrated to?	

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.1 System Documentation: hardware procurement			
1.A.1 System Documentation: hardware installation			
1.A.1 System Documentation: hardware modifications			
1.A.1 System Documentation: hardware maintenance			
1.A.1 System Documentation: use of only agency-authorized hardware			
1.A.2 System Documentation: software procurement			
1.A.2 System Documentation: software installation			
1.A.2 System Documentation: software modification			
1.A.2 System Documentation: software maintenance			
1.A.2 System Documentation: use of only agency-authorized software			
1.A.3 System Documentation: communication networks procurement			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.3 System Documentation: communication networks installation			
1.A.3 System Documentation: communication networks modifications			
1.A.3 System Documentation: communication networks maintenance			
1.A.4 System Documentation: interconnected systems (including the Internet) — list			
1.A.4 System Documentation: interconnected systems — names and unique identifiers			
1.A.4 System Documentation: interconnected systems — owners			
1.A.4 System Documentation: interconnected systems — names and titles of authorizing personnel			
1.A.4 System Documentation: interconnected systems — dates of authorization			
1.A.4 System Documentation: interconnected systems — types of connections			
1.A.4 System Documentation: interconnected systems — indication of system of record			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.A.4 System Documentation: interconnected systems — sensitivity levels			
1.A.4 System Documentation: interconnected systems — security mechanisms, security concerns, personnel rules of behavior			
1.B.1 System Documentation: programming conventions and procedures			
1.B.2 System Documentation: development and testing procedures, including tools			
1.B.2 System Documentation: development and testing procedures — periodic functional tests should include anomalous as well as routine conditions and be documented such that they are repeatable			
1.B.3 System Documentation: applications and associated procedures for entering and accessing data			
1.B.3 System Documentation: applications and associated procedures for data modification			
1.B.3 System Documentation: applications and associated procedures for data duplication			
1.B.3 System Documentation: applications and associated procedures for data deletion			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.B.3 System Documentation: applications and associated procedures for indexing techniques			
1.B.3 System Documentation: applications and associated procedures for outputs			
1.B.4 System Documentation: identification of when records become official			
1.B.5 System Documentation: record formats and codes			
1.B.6 System Documentation: routine performance of system backups — appropriate labels			
1.B.6 System Documentation: routine performance of system backups — secure, off-line, off-site storage			
1.B.6 System Documentation: routine performance of system backups — periodic integrity tests			
1.B.7 System Documentation: routine performance of quality assurance and control checks (incl. audit trails)			
1.B.7 System Documentation: routine performance of quality assurance and control checks — identification devices (e.g., security cards) periodically checked to ensure proper functioning and correctness of identifying information and system privilege levels			

Criteria Group 1 Checklist (1.A-1.B.)

System Documentation Analysis (e.g., specifications, program manuals, user guides) included in retention schedules, retained for as long as the longest retention time applicable to the records produced in accordance with the documents

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
1.B.7 System Documentation: routine performance of quality assurance and control checks — storage mediums undergo regular statistical sampling following established procedures outlining sampling methods, identification of data loss and corresponding causes, and the correction of identified problems			
1.B.8 System Documentation: migration of records to new systems and media as necessary, with all record components managed as a unit throughout transfer			
1.B.9 System Documentation: standard training for all users and personnel with access to equipment			
1.B.9 System Documentation: standard training — users should sign statements agreeing to terms of use			

Criteria Group 2: System Security System Security Questions	Response
Who can invoke change mechanisms for object, process, and user security levels?	
Who (creator, current owner, system administrator, etc.) can grant access permission to an object after the object is created?	
Is there a help desk or group that offers advice and can respond to security incidents in a timely manner?	
Is system performance monitoring used to analyze system performance logs in real-time to look for availability problems, including active attacks and system and network slowdowns and crashes?	
List internal and external user groups and the types of data created and accessed.	
Have all positions been reviewed with respect to appropriate security levels?	
What are the procedures for the destruction of controlled-access hardcopies?	
How is information purged from the system?	
How is reuse of hardware, software, and storage media prevented?	

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.1 System Security — User Authorization: user identification and access procedures should be established and documented			
2.A.1 System Security — User Authorization: users should be authenticated prior to being granted access			
2.A.2 System Security — User Authorization: unique identifier and password for each user			
2.A.2 System Security — User Authorization: identifiers and passwords not used more than once within a system			
2.A.2 System Security — User Authorization: use of access scripts with embedded passwords limited and controlled			
2.A.2 System Security — User Authorization: upon successful log-in, users should be notified of date and of last successful log-in, location of last log-in, and each unsuccessful log-in attempt on user identifier since last successful entry			
2.A.2 System Security: where identification codes in human-readable form are too great a security liability, use of other forms such as encoded security cards or biometric-based devices			
2.A.3 System Security — User Authorization: password rules include minimum password length, expiration dates, and limited number of log-on attempts			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.3 System Security — User Authorization: determination of what level and frequency of log-on error constitutes a misuse problem which, in turn, would trigger notification of security personnel			
2.A.4 System Security — User Authorization: users restricted to only level of access necessary to perform their job duties			
2.A.5 System Security — User Authorization: permission to alter disposition/retention codes, and/or to create, modify, and delete records granted only to authorized users with proper clearance			
2.A.5 System Security — User Authorization: modification of record identifiers prohibited			
2.A.6 System Security — User Authorization: Access to private keys for digital signatures limited to authorized personnel			
2.A.7 System Security — User Authorization: maintenance of lists of all current and past authorized users along with their privileges and responsibilities			
2.A.7 System Security — User Authorization: current list of users reviewed on a regular schedule to ensure timely removal of authorizations for former employees, and adjustment of clearances for workers with new job duties			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.A.8 System Security — User Authorization: personnel duties and access restrictions arranged such that no individual with an interest in record content will be responsible for administering system security, quality controls, audits, or integrity-testing functions.			
2.A.8 System Security — User Authorization: No individual should have the ability to single-handedly compromise the system's security and operations			
2.B.1 Internal System Security: access to system documentation controlled and monitored			
2.B.2 Internal System Security: access to output and storage devices controlled and monitored			
2.B.3 Internal System Security: controls in place to ensure proper security levels of data when archiving, purging, or moving from system to system			
2.B.3 Internal System Security: controls in place for the transportation or mailing of media or printed output			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of hardware when no longer needed.			
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of software when no longer needed			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.B.4 Internal System Security: procedures for the complete sanitization and secure disposal of storage media when no longer needed			
2.B.4 Internal System Security: documentation of sanitization and secure disposal should include date, equipment identifiers, methods, personnel names			
2.B.5 Internal System Security — insecurity-detection mechanisms constantly monitoring the system			
2.B.5 Internal System Security: fail-safes and processes to minimize the failure of primary security measures in place at all times			
2.B.6 Internal System Security: security procedures and rules reviewed on a routine basis to maintain currency			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — access to rooms with terminals, servers, wiring, backup media			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — data interception			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — mobile/portable units such as laptops			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — structural integrity of building			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — fire safety			
2.B.7 Internal System Security — Access: measures in place to guard system's physical security — supporting services such as electricity, heat, air conditioning, water, sewage, etc.			
2.B.8 Internal System Security: security administration personnel undergo training to ensure full understanding of the security system's operation			
2.C.1 External System Security: additional security measures employed in cases of remote access, especially through public telephone lines (e.g., input device checks, caller identification checks (phone caller identification), callbacks, security cards)			
2.C.2 External System Security: for records originating outside of the system, the system should be capable of verifying their origin and integrity			
2.C.2 External System Security: non-system records — verification of sender or source			
2.C.2 External System Security: non-system records — verification of the integrity, or detection of errors in the transmission or informational content of record			

Criteria Group 2 Checklist (2.A-2.C.)
System Security Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
2.C.2 External System Security: non-system records — detection of changes in the record since the time of its creation or the application of a digital signature			
2.C.2 External System Security: non-system records — detection of viruses or worms			

Criteria Group 3: Audit Trails Audit Trail Questions	Response
Who can access audit data?	
Who can alter audit data?	
Who can add audit data?	
Who can delete audit data?	
How can the audit logs be read?	
Who can read audit data?	
What tools are available to output audit information? What are the formats?	
Who can output audit information?	
What mechanisms are available to designate and change activities chosen for audit?	
Who is able to designate and change activities chosen for audit?	
How are audit logs protected?	

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.A Audit Trails: if audit trails are encoded to conserve space, the decode mechanism must always accompany the data			
3.A.1 Audit Trails — General Characteristics: audit trail software and mechanisms subject to strict access controls			
3.A.1 Audit Trails — General Characteristics: audit trail software and mechanisms protected from unauthorized modification			
3.A.1 Audit Trails — General Characteristics: audit trails protected from circumvention			
3.A.2 Audit Trails — General Characteristics: audit trails backed up periodically onto removable media to ensure minimal data loss in case of system failure			
3.A.3 Audit Trails — General Characteristics: system automatically notifies system administrators when audit storage media nearing capacity. Response documented			
3.A.3 Audit Trails — General Characteristics: when storage media containing audit trail is physically removed from the system, the media should be physically secured as required by the highest sensitivity level of the data it holds			
3.B Audit Trails — System to track password Usage and Changes			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.B Audit Trails — Password Usage and Changes: user identifier			
3.B Audit Trails — Password Usage and Changes: successful and unsuccessful log-ins			
3.B Audit Trails — Password Usage and Changes: use of password-changes procedures			
3.B Audit Trails — Password Usage and Changes: user ID lock-out record			
3.B Audit Trails — Password Usage and Changes: date of password use			
3.B Audit Trails — Password Usage and Changes: time of password use			
3.B Audit Trails — Password Usage and Changes: physical location of user			
3.C Audit Trails — Users: system in place to log and track users and their online actions			
3.C Audit Trails — Users: system in place to log and track users and their online actions — details of log-in (date, time, physical location, etc.)			
3.C Audit Trails — Users: system in place to log and track users and their online actions — creation of files/ records			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.C Audit Trails — Users: system in place to log and track users and their online actions — accessed file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level, etc.)			
3.C Audit Trails — Users: system in place to log and track users and their online actions — accessed device identifiers			
3.C Audit Trails — Users: system in place to log and track users and their online actions — software use			
3.C Audit Trails — Users: system in place to log and track users and their online actions — production of printed output			
3.C Audit Trails — Users: system in place to log and track users and their online actions — overriding of human-readable output markings (including overwrite of sensitivity label markings and turning-off of labeling mechanisms) on printed output			
3.C Audit Trails — Users: system in place to log and track users and their online actions — output to storage devices			
3.C Audit Trails — Users: users made aware that their use of computerized resources is traceable			

Criteria Group 3 Checklist (3.A-3.D.)
Audit Trail Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
3.D Audit Trails: Logged for each record by audit trails: user identifier			
3.D Audit Trails: Logged for each record by audit trails: record identifier			
3.D Audit Trails: Logged for each record by audit trails: date			
3.D Audit Trails: Logged for each record by audit trails: time			
3.D Audit Trails: Logged for each record by audit trails: usage (e.g., creation, capture, retrieval, modification, deletion)			

Criteria Group 4: Checklist
Disaster Planning and Recovery

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
4.A Disaster Plan: periodically reviewed for currency and tested for efficiency			

Criteria Group 5: Metadata Metadata Questions	Response
What are the current components of a complete or final record of the transaction?	
What are the minimal components necessary to provide evidence of the transaction? (If you went to court, what would be the minimum information you would need?)	
Are there any laws, regulations, or professional best practices that specify the structure (including medium, format, relationships) of the record of the transaction or any of its components?	
What information is necessary to interpret the contents of the record?	
During which agency business processes might you have to access this record?	
Who are the external secondary users of the record?	
What are the rules, laws, and regulations that restrict or open access to these records to external users?	
How will the record be reproduced to meet the needs of internal and external secondary users? What are the reproduction formats?	
Is there a mechanism in place to indicate sensitivity level on hardcopies? Who can enable/disable this function?	
What are your industry's standards for records retention?	
What is the records disposition plan?	
Who is responsible for authorizing the disposition of records?	
Who is responsible for changes to the records disposition plan?	

Criteria Group 5: Metadata Metadata Questions	Response
How does the system accommodate integration of records from other systems?	
Who can access metadata?	
Who can alter metadata?	
Who can delete metadata?	
Who can add metadata?	
Does system automatically assign unique consecutive numbers and time-date stamps to the individual units of storage media as they are written to for the first time to prevent the addition of false units or the removal of legitimate ones from the storage series?	
Does the system automatically assign new identifiers to modified records?	
If the records are not individually authenticated, does the record series metadata include the name or title of the individual responsible for validating or confirming the data within the record series and for confirming that the particular series was produced in accordance with standard procedures?	

Criteria Group 5: Checklist (5.A)
Metadata Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
5.A.1 Record metadata: unique identifier			
5.A.2 Record metadata: date of creation			
5.A.3 Record metadata: time of creation			
5.A.4 Record metadata: creator/agency/organization			
5.A.5 Record metadata: documentation of creator's authorization			
5.A.6 Record metadata: date of modification			
5.A.7 Record metadata: time of modification			
5.A.8 Record metadata: modifier/agency/organization			
5.A.9 Record metadata: documentation of modifier's authorization			
5.A.10 Record metadata: indication of authoritative version			
5.A.11 Record metadata: identification of originating system			
5.A.12 Record metadata: date of receipt from outside system			
5.A.13 Record metadata: time of receipt from outside system			
5.A.14 Record metadata: addressee			
5.A.15 Record metadata: system or mechanism used to capture record from outside system			

Criteria Group 5: Checklist (5.A)
Metadata Analysis

Criteria	In Place? Yes/No	Planned? Yes/No	Rationale/Notes
5.A.16 Record metadata: protection method			
5.A.17 Record metadata: media type			
5.A.18 Record metadata: format			
5.A.19 Record metadata: location of record			
5.A.20 Record metadata: sensitivity classification			

Data Warehousing Questions	Response
Do you gather extraction metadata?	
Do you cleanse the data?	
Do you document the cleansing procedure?	
Do you gather cleansing metadata?	
Do you transform the data?	
Do you document the transformation procedure?	
Do you gather transformation metadata?	
What metadata/documentation do you offer users?	
Who can access metadata?	
Who can alter metadata?	
Who can delete metadata?	
Who can add metadata?	
What are the legal liabilities regarding data ownership and custodial responsibilities?	
Where do data custody responsibilities reside — with the source systems, the warehouse system, or both?	
Are there records retention schedules and policies for warehouse data?	
Is retention of warehouse data coordinated with retention of data in the source systems?	

Appendices

The following appendices complement the material found in the main body of the Handbook.

A1 Glossary
Defines terms that are used throughout the *Handbook*

A2 Bibliography
Provides citations to works consulted during *Handbook* development

A3 Citation
Citation of the *Trustworthy Information Systems Handbook*

A4 Background Information
Background of the Trustworthy Information Systems Project

A5 Methodology
Trustworthy Information Systems Project Methodology

A6 South Carolina Laws, Standards, and Guidelines
South Carolina Laws, Standards, and Guidelines Relating to Electronic Records

A7 Legal Issues
Legal Issues Affecting Electronic Records Management

Appendix 1: Glossary

Note: Definition sources are indicated by letters and listed at the end.

Accountability 1. The quality of being responsible, answerable; the obligation to report, explain, or justify an event or situation.

Archival Value 1. "The values, evidential and/or informational that justify the continuing retention of records as archives." (h)

Archiving 1. "The process of creating a backup copy of computer files, especially for long-term storage." (g)

Asymmetric Encryption 1. "A form of cryptosystem in which encryption and decryption are performed using two different keys, one of which is referred to as the public key and one of which is referred to as the private key. Also known as public-key encryption." (a)

Audit Trail 1. "A record showing who has accessed a computer system and what operations he or she has performed during a given period of time." (b)

Authenticity 1. Authenticity is a function of a record's preservation and is a measure of a record's reliability over time.

Authentication 1. "A process used to verify the integrity of transmitted data, especially a message." (a)

2. "The process of identifying an individual, usually based on a username and password. In security systems, authentication is distinct from authorization, which is the process of giving individuals access to system objects based on their identity. Authentication merely ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual." (b)

3. "The process of confirming an asserted identity with a specified, or understood, level of confidence. The mechanism can be based on something the user knows, such as a password, something the user possesses, such as a 'smart card,' something intrinsic to the person, such as a fingerprint, or a combination of two or more of these." (f)

Back-up 1. "To copy files to a second medium . . . as a precaution in case the first medium fails." (b)

Backup 1. "A substitute or alternative. The term backup usually refers to a disk or tape that contains a copy of data." (b)

Biometric-based Device 1. An authentication technique relying on measurable physical characteristics of the user that can be automatically checked. An example is a fingerprint scanner. (b)

Data 1. "Symbols, or representations, of facts or ideas that can be communicated, interpreted, or processed by manual or automated means." (g)

Data Model 1. A diagram that shows the various subjects about which information is stored, and the relationships between those subjects.

Data Warehouse 1. A computer-based information system that is home for "secondhand" data that originated from either another application or from an external system or source. A data warehouse is a read-only, integrated database designed to answer comparative and "what if" questions. Unlike operational databases that are set up to handle transactions and that are kept up to date as of the last transaction, a data warehouse is analytical, subject-oriented, and structured to aggregate transactions as a snapshot in time.

Digital 1. "Describes any system based on discontinuous data or events. Computers are digital machines because at their most basic level they can distinguish between just two values, 0 and 1, or off and on. There is no simple way to represent all the values in between, such as 0.25. All data that a computer processes must be encoded digitally, as a series of zeroes and ones." (b)

Digital Signature 1. "An authentication mechanism that enables the creator of a message to attach a code that acts as a signature. The signature guarantees the source and integrity of the message." (a) *See also "Electronic Signature"*

Disaster 1. "An unexpected occurrence inflicting widespread destruction and distress and having long-term adverse effects on agency operations. Each agency defines what a long-term adverse effect is in relation to its most critical program." (g)

Documentation 1. "The act or process of substantiating by recording actions and/or decisions." (g)

2. "Records required to plan, develop, operate, maintain, and use electronic records. Included are systems specifications, file specifications, codebooks, file layouts, user guides, and output specifications." (g)

Dynamic 1. "Refers to actions that take place at the moment they are needed rather than in advance." (b)

Electronic 1. "Of, or relating to, technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." (d)

Electronic Document 1. "Recorded information that is recorded in a form that requires a computer or other machine to process it. Includes word processing documents; electronic mail messages; . . . internet and intranet postings; numerical and textual spreadsheets and databases; electronic files; optical images; software; and information systems." (g)

Electronic Record 1. "A record created, generated, sent, communicated, received, or stored by electronic means." (i)

Electronic Signature 1. "In South Carolina, an 'Electronic signature' means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record." (i) *See also "Digital Signature"*

Firewall 1. "A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized internet users from accessing private networks connected to the internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria." (b)

Format 1. "The shape, size, style, and general makeup of a particular record." (g)

Hard Copy 1. "A printout of data stored in a computer. It is considered hard because it exists physically on paper, whereas a soft copy exists only electronically." (b)

Information 1. Data, text, images, sounds, codes, computer programs, software, databases, etc. (d)

Information System 1. "An electronic system for creating, generating, sending, receiving, storing, displaying, or otherwise processing information." (d)
2. "The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual. . . . Most often refers to a system containing electronic records, which involves input or source documents, records on electronic media, and output records, along with related documentation and any indexes." (g)

Input Device 1. Any apparatus, such as a keyboard, that allows data to be fed or entered into a computer. (b)

Internet 1. A decentralized global network connecting millions of computers.

Intranet 1. "A network . . . belonging to an organization . . . accessible only by the organization's members, employees, or others with authorization. An intranet's websites look and act just like any other websites, but the firewall surrounding an intranet fends off unauthorized access." (b)

Legacy System 1. "An application in which a company or organization has already invested considerable time and money." (b)

Log-in 1. To enter information before gaining access to a computer system. At the minimum, log-in typically requires a username and password.

Metadata 1. Data about data.
2. "The description of the data resources, its characteristics, location, usage, and so on. Metadata is used to identify, describe, and define user data." (g)

Microform 1. "Any form containing greatly reduced images, or microimages, usually on microfilm. Roll, or generally serialized, microforms include microfilm on reels, cartridges, and cassettes. Flat, or generally unitized, microforms include microfiche, microfilm jackets, aperture cards, and microcards, or micro-opaques." (g)

Migration 1. The process of moving computer files from one information system or medium to another.

Official Record 1. "In disposal scheduling, the copy of the record held by the office of record. Any other copies of the record can then be destroyed whenever they are no longer required." (h)

Output Device 1. Any machine capable of representing information from a computer, including display screens, printers, plotters, and synthesizers. (b)

Password 1. "A character string used to authenticate an identity. Knowledge of the password and its associated user ID is considered proof of authorization to use the capabilities associated with that user ID." (a)

Permanent Value *See "Archival Value"*

Private Key 1. "One of the two keys used in an asymmetric encryption system. For secure communication, the private key should be known only to its creator." (a)

Public Key 1. "One of the two keys used in an asymmetric encryption system. The public key is made public, to be used in conjunction with a corresponding private key." (a)

Public Record 1. In South Carolina, a "public record" includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body." (e) *See also "Record"*

Record 1. "Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." (i)
2. Information created or received during the course of government business that becomes part of an official transaction. *See also "Public Record"*

Reliability 1. Reliability is the measure of a record's authority and is determined solely by the circumstances of the record's creation.

Removable Media 1. Media, such as tapes, floppy disks, and CD ROMs, that can be physically removed from the computer environment.

Retention Period 1. "The period of time, usually based on an estimate of the frequency of current and future use, and taking into account statutory and regulatory provisions, that records need to be retained before their final disposal." (h)

Retention Schedule 1. A document that describes records by series, specifies the length of time required for their maintenance, and provides instruction for their final disposition. **General schedules**, designed for records that are common to many government offices, and **specific schedules**, designed for records that are unique to one government office, can be applied to agency records.

Risk Analysis 1. A component of risk management that evaluates risks (the possibility of incurring loss or injury), examining the probability of loss or injury occurring, then determining the amount of risk that is acceptable for a given situation or event; a prioritization of risks.

Spoliation 1. The destruction of evidence.

Storage Device 1. A device capable of storing data such as disk drives and tape drives. (b)

System Development Life Cycle 1. "A systematic and orderly approach to solving business problems, and developing and supporting resulting information systems." Typical phases of the system development life cycle include: Planning, Analysis, Design, Implementation, and Support. (c)

Transaction 1. "An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs." (i)

Trustworthy 1. An information system that produces reliable and authentic records.

URL 1. "Abbreviation of Uniform Resource Locator, the global address of documents and other resources on the World Wide Web." (b)

Virus 1. "Code embedded within a program that causes a copy of itself to be inserted in one or more other programs. In addition to propagation, the virus usually performs some unwanted function." (a)

World Wide Web (WWW) 1. "A system of Internet servers that support specially formatted documents. The documents are formatted in a language called HTML (HyperText Markup Language) that supports links to other documents, as well as graphics, audio, and video files." (b)

Worm 1. "Program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again. In addition to propagation, the worm usually performs some unwanted function." (a)

Sources

a. William Stallings, *Cryptography and Network Security: Principles and Practice*. Upper Saddle River, NJ: Prentice Hall, 1999.

b. Webopedia. [http://webopedia.internet.com/]. November 1999.

c. Jeffrey L. Whitten, Lonnie D. Bentley, and Victor M. Barlow, *System Analysis and Design Methods*. Burr Ridge, IL: Irwin, 1994.

d. National Conference of Commissioners on State Laws, *Draft: Uniform Electronic Transactions Act*. [www.law.upenn.edu/library/ulc/ulc.htm]. March 1999.

e. State of California, *Uniform Electronic Transactions Act*. November 1999.

f. Fred B. Schneider, ed., *Trust in Cyberspace*. Committee on Information Systems Trustworthiness, National Research Council. Washington, D.C.: National Academy Press, 1999.

g. U.S. Environmental Protection Agency, "Glossary of Common Records Management Terms." [www.epa.gov/records/gloss/index.htm]. November 1999.

h. Minnesota Statutes, Chapter 13, Section 13.04, Subdivision 2.

i. Judith Ellis, ed., *Keeping Archives, Second Edition*. Port Melbourne, Victoria, Australia: D.W. Thorpe, in association with The Australian Society of Archivists, Inc., 1997.

i. State of South Carolina, *Electronic Commerce Act*. May 1998.

Appendix 2: Bibliography

South Carolina: Directives, Policies, Procedures, and Rules

South Carolina Department of Archives and History Information leaflets
[www.state.sc.us/scdah/techlflt.htm#leaflets]

Leaflet #13: Public Records Stored as Digital Images: Policy Statement

South Carolina Department of Archives and History Electronic Records Management Guidelines
[www.state.sc.us/scdah/erg/erg.htm]

Introduction
Records Management in an Electronic Environment
File Naming
File Formats
Digital Media
Digital Media Storage — Facilities and Procedures
Electronic Document Management Systems
Digital Imaging
E-mail Management
Web Content Management
Electronic and Digital Signatures
Trustworthy Information Systems Handbook
Glossary

South Carolina Division of the CIO

Creating an IT Blueprint for State Government
[www.cio.sc.gov/textonly/cioContent.asp?pageID=389&menuID=297]

South Carolina: Laws

Code of Laws of South Carolina: [www.scstatehouse.net/code/statmast.htm]

South Carolina Public Records Act [www.state.sc.us/scdah/praf.htm]
South Carolina Electronic Commerce Act [www.state.sc.us/intranet/oir/meet/coi/ec/sceca.html]

Other States: Guidelines, Reports, and Laws

Delaware. Delaware Public Archives. *Model Guidelines for Electronic Records*. 20 January 1998.

New York. New York State Archives and Records Administration. *Guidelines for the Legal Acceptance of Public Records in an Emerging Electronic Environment*. 1994.
[www.nysl.nysed.gov/scandoclinks/ocm31941498.htm]

Federal Government: Guidelines, Reports, and Laws

U.S. Public Law 106-229. 106th Congress, 2nd Session, 30 June 2000. *Electronic Signatures in Global and National Commerce Act*. [http://thomas.loc.gov/]

Commodity Futures Trading Commission. *Recordkeeping*. Proposed Rule (17 CFR Part 1) in *Federal Register* (5 June 1998) vol. 63, no. 108, 30668-30675. [www.gpoaccess.gov/nara/index.html]

National Archives and Records Administration. *Electronic Records Management*. *Code of Federal Regulations*, Chapter 12, Title 36, Part 1234. [www.gpoaccess.gov/cfr/index.html]

U.S Department of Commerce. Patent and Trademark Office. *Checklist of Requirements for Electronic Records Management (ERM) Over the Life Cycle of Patent and Trademark Records*. Prepared by Cohasset Associates, Inc., 26 February 1999.

U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology.

CS2: Protection Profile Guidance for Near-Term COTS, (Draft Version 0.5), and *Rationale for CS2: Protection Profile Guidance for Near-Term COTS*, (Draft Version 0.5), by Gary Stoneburner. 25 March 1999. Re-titled as, and superseded by, *CSPP — Guidance for COTS Security Protection Profiles*, (Version 1.0, NISTIR 6462), January 2000.

An Introduction to Computer Security: The NIST Handbook. NIST Special Publication 800-12. October 1995. [http://csrc.nist.gov/publications/nistpubs/index.html]

Generally Accepted Principles and Practices for Securing Information Technology Systems, by Marianne Swanson and Barbara Guttman. NIST Special Publication 800-14. September 1996. [http://csrc.nist.gov/publications/nistpubs/index.html]

U.S. Department of Commerce. Technology Administration. National Institute of Standards and Technology, Federal Computer Security Program Managers' Forum Working Group. *Guide for Developing Security Plans for Information Technology Systems*, by Marianne Swanson. NIST Special Publication 800-18. December 1998. [http://csrc.nist.gov/publications/nistpubs/index.html]

U.S. Department of Defense.

Design Criteria for Electronic Records Management Software. Prepared by the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. DoD 5015.2-STD. November 1997, Revised June 2002. [http://jitc.fhu.disa.mil/recmgt/standards.htm]

Department of Defense Trusted Computer System Evaluation Criteria. DoD 5200.28-STD. December 1985. [http://csrc.nist.gov/secpubs/rainbow/std001.txt]

Password Management Guideline. CSC-STD-002-85. 12 April 1985. [www.fas.org/irp/nsa/rainbow/std002.htm]

U.S. Department of Defense. National Computer Security Center.

A Guide to Understanding Audit in Trusted Systems. NCSC-TG-001. 1 June 1988. [www.fas.org/irp/nsa/rainbow/tg001.htm]

A Guide to Understanding Configuration Management in Trusted Systems. NCSC-TG-006-88. 28 March 1988.

A Guide to Understanding Identification and Authentication in Trusted Systems. NCSC-TG-017. September 1991. [http://packetstormsecurity.nl/docs/rainbow-books/NCSC-TG-017.txt]

Trusted Network Interpretation of the TCSEC (TNI). NCSC-TG-005. 31 July 1987. [www.fas.org/irp/nsa/rainbow/tg005.htm]

Trusted Product Evaluation Questionnaire. 2 May 1992. [www.fas.org/irp/nsa/rainbow/tg002.htm]

Integrity in Automated Information Systems, by Terry Mayfield, J. Eric Roskos, Stephen R. Welke, and John M. Boone. C Technical Report 79-91. September 1991. [www.iwar.org.uk/comsec/resources/standards/rainbow/C-TR-79-91.htm]

U.S. Department of Defense. National Security Agency. National Telecommunications and Automated Information Systems Security Committee. *Advisory Memorandum on Office Automation Security Guidelines*. NTISSAM COMPUSEC 1-87. 1987. [www.iwar.org.uk/comsec/resources/standards/rainbow/N-C-1-87.htm]

U.S. Department of Energy. *Records Considerations for Electronic Information: Guidelines for Individuals and Systems Administrators*. Prepared by the Lockheed Martin Energy Systems Electronic Records Committee for the Oak Ridge National Laboratory. February 1996.

U.S. Department of Health and Human Services. *Security and Electronic Signature Standards [as related to Health Insurance Portability and Accountability Act of 1996]*. Proposed Rule (45 CFR Part 142) in *Federal Register* (12 August 1998) vol. 63, no. 155, 43241-43280. [www.gpoaccess.gov/nara/index.html]

U.S. Department of Health and Human Services. Food and Drug Administration. *Electronic Records; Electronic Signatures. Code of Federal Regulations*, Chapter 1, Title 21, Part 11. Final Rule in *Federal Register* (20 March 1997) vol. 62, no. 54, 13430-13466. [www.gpoaccess.gov/nara/index.html]

U.S. Department of Justice. *National Criminal Background Check System Regulations*. Proposed Rule (28 CFR Part 25) in *Federal Register* (4 June 1998) vol. 63, no. 107, 30430-30438. [www.gpoaccess.gov/nara/index.html]

U.S. Department of Treasury. Customs Service. *Recordkeeping Requirements. Code of Federal Regulations*, Chapter 1, Title 19, Parts 19, 24, 111, 113, 143, 162, 163, 178, and 181. Final Rule in *Federal Register* (16 June 1998) vol. 63, no. 115, 32916-32955. [www.gpoaccess.gov/nara/index.html]

U.S. Department of Treasury. Internal Revenue Service. *Revenue Procedure 98-25*. 1998.

"Retention of Books and Records: Section 4 — Electronic Storage System Requirements." *Revenue Procedure 97-22*. 1997.

International Government: Guidelines, Reports, and Laws

Australia. Australian Archives (National Archives of Australia). *Keeping Electronic Records: Policy for Electronic Recordkeeping in the Commonwealth Government*. September 1995. Now part of NAA's expanded online offerings for the Commonwealth Recordkeeping Program. [www.naa.gov.au/recordkeeping/overview/summary.html]

Australia. Defence Signals Directorate.

Australian Communications — Electronic Security Instructions 33 (ACSI 33): Security Guidelines for Australian Government IT Systems. April 1998. [www.dsd.gov.au/library/infosec/acsi33.html]

Australian Communications — Electronic Security Instructions 38 (ACSI 38): Australian Government Standards for the Protection of Electronic Business Systems and Internet Delivery Mechanisms. 9 February 1999.

Australia. State of Victoria, Public Records Office. *Victorian Electronic Records Strategy Final Report*. 1998. [www.prov.vic.gov.au/vers/pdf/final.pdf]

Great Britain. Public Record Office.

Management, Appraisal and Preservation of Electronic Records — Vol. I: Principles. 1999. [www.nationalarchives.gov.uk/recordsmanagement/]

Management, Appraisal and Preservation of Electronic Records — Vol. II: Procedures. 1999. [www.nationalarchives.gov.uk/recordsmanagement/]

National Organizations: Guidelines and Reports

American Bar Association, Internal Security Committee, Electronic Commerce and Information Technology Division, Section of Science and Technology. *Digital Signature Guidelines: Legal Infrastructure for Certification Authorities and Secure Electronic Commerce*. 1 August 1996. [www.abanet.org/scitech/ec/isc/dsgfree.html]

Association for Information and Image Management.
The following reports are available for purchase at www.aiim.org

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems — Part I: Performance Guideline for Admissibility of Records Produced by Information Technology Systems as Evidence. AIIM Report No. TR31-1992. 1992.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems — Part II: Performance Guideline for the Acceptance by Government Agencies of Records Produced by Information Technology Systems. ANSI/AIIM Report No. TR31-1993. 1993.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems — Part III: Implementation of the Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems. ANSI/AIIM Report No. TR31-1994. 1994.

Performance Guideline for the Legal Acceptance of Records Produced by Information Technology Systems — Part IV: Model Act and Rule. ANSI/AIIM Report No. TR31-1994. 1994.

Information Systems Audit and Control Association and Foundation. *COBIT: Control Objectives for Information and Related Technology*. 1998. [www.isaca.org/cobit.htm]

International Federation of Accountants, Information Technology Committee. *International Information Technology Guideline: Managing Security of Information*. January 1998.

National Conference of Commissioners on Uniform State Laws. *Draft: Uniform Electronic Transactions Act*. 19 March 1999. [www.law.upenn.edu/library/ulc/ulc.htm]

Nuclear Information and Records Management Association.
The following reports are available at www.nirma.org

Authentication of Records and Media (Report No. TG11-1998). 1998.

Electronic Records Protection and Restoration (Report No. TG21-1998). 1998.

Management of Electronic Records (Report No. TG15-1998). 1998.

Software Configuration Management and Quality Assurance (Report No. TG16-1998). 1998.

Electronic Records Projects and Studies

Center for Technology in Government (Albany, New York). *Models for Action: Developing Practical Approaches to Electronic Records Management and Preservation*. 1998. [www.ctg.albany.edu/projects/er/ermn.html]

Duranti, Luciana, Terry Eastwood, and Heather MacNeil. *The Preservation of the Integrity of Electronic Records*. 1997. [www.interpares.org/UBCProject/index.htm]

Indiana University Archives. *Indiana University Electronic Records Project, 1995-1997: Final Report to the National Historical Publications and Records Commission (NHPRC)*. April 1998. [www.libraries.iub.edu/index.php?pageID=3313]

University of Pittsburgh, School of Information Sciences. *Functional Requirements for Evidence in Recordkeeping*. 1996. [www.archimuse.com/papers/nhprc/prog1.html]

Appendix 3: Citation of the *Trustworthy Information Systems Handbook*

Users should be aware of the following information as they refer to the *Trustworthy Information Systems Handbook:*

- Versions are identified by number.
- New versions will be released as substantive changes are made to sections other than the bibliography (which changes on a continual basis). The most current version will always be online.
- Past versions will be kept in PDF format by the South Carolina Department of Archives and History for five years and will be made available by request. Users concerned about ongoing access to a particular version (e.g., for audit purposes) should download and maintain within their own agency the PDF of the entire handbook.
  - *Version 1* (January 2004 – March 2007)
  - *Version 2* (March 2007 –)

Users wishing to cite the *Handbook* should use the following format:

South Carolina Department of Archives and History. *Trustworthy Information Systems Handbook*. Version 2, March 2007.

Appendix 4: Background of the Trustworthy Information Systems Project

South Carolina

The South Carolina *Trustworthy Information Systems Handbook* (TIS) is based on the Minnesota Historical Society's Trustworthy Information Systems (TIS) project [www.mnhs.org/preserve/records/tis/tis.html]. This endeavor by the South Carolina Department of Archives and History (SCDAH) to improve electronic records management stems from consultant Timothy Slavin's 1999 assessment of electronic records activity in the Department. Several grants from the NHPRC permitted the SCDAH to begin laying the groundwork for an electronic records program. Establishment of a project team in January 2003 and the addition of a project archivist in June commenced the exploration and adaptation of this *Handbook* for the benefit of South Carolina government agencies. The South Carolina Department of Archives and History will keep the South Carolina TIS up to date. The most current version will always be available on the SCDAH website.

Minnesota

The Minnesota Trustworthy Information Systems (TIS) project grew out of a grant to the Minnesota State Archives from the National Historical Publications and Records Commission to establish an electronic records program. The funding was used, in part, to hire an additional staff person, and work got underway in March 1998.

The first two phases of the project involved developing the criteria set and testing it for practicality against actual government information systems (refer to Appendix F). State Archives staff promoted the TIS project and sought collaborators by giving talks to government entities and by offering an informational brochure. By October 1999, the State Archives had worked with the following agencies: the Minnesota Housing Finance Agency; the Minnesota Department of Finance; the Minnesota Department of Children, Families and Learning; the Minnesota Department of Transportation; and the City of Minneapolis.

Phases three and four of the project are implementation and education. Implementation centers around web-enabled delivery of TIS products. Early on, a general discussion of trustworthy information systems, the criteria set, and the bibliography were made available on the State Archives' World Wide Web site. With sponsorship from the IPC and in consultation with Signorelli & Associates, Inc., a Saint Paul-based technical writing firm, these items were enhanced and re-worked into the present handbook for wide distribution to government agencies.

Appendix 5: Trustworthy Information Systems Project Methodology

South Carolina

A project team established at South Carolina Department of Archives and History (SCDAH) began examining the Minnesota Historical Society's TIS Handbook in 2003. The team revised the document to reflect South Carolina law and policies and completed version 1 in July 2004.

Version 2 resulted from the need to make a number of corrections to the web links that were no longer working, to remove from the criteria checklist one item that was not applicable to South Carolina, to delete references to SCDAH publications no longer in use, to add references to new publications, guidelines, and standards, and to include information on the 2006 revisions to the Federal Rules of Civil Procedure.

Minnesota

Minnesota State Archives' work on the Trustworthy Information Systems project got fully underway in March 1998 and advanced in two phases, culminating in the production of this handbook.

The first phase consisted of researching and compiling the criteria set. A wide range of sources concerned with legal, audit, records management, and archival requirements and standards were surveyed (refer to the *Bibliography*). Common items of concern in each area came together in the criteria set, which stands within the particular framework of Minnesota's laws and policies.

Once the criteria set was in draft form, attention turned to field testing with respect to actual government information systems. Over the course of the testing phase, the set was applied to five different systems. In each case, State Archives staff met with agency personnel knowledgeable about the particular system under scrutiny and led the examination process. One State Archives staff member walked the group, item-by-item, through the criteria while another transcribed the interview information into a chart on a laptop computer. Participants were queried as to whether each criterion was considered important and whether it was currently implemented or planned for future implementation. With each system, the criteria set was supplemented with general questions relevant to that particular function and/or agency. Results were shared with each agency for review and comment as well as for its own internal use.

The findings from the testing phase formed the basis for the formalized process for determining the trustworthiness of information systems presented in this handbook. As the criteria set is applied to more systems, State Archives staff anticipate that the examination process will be refined and that new versions of the handbook will be released as necessary. Additionally, the criteria set will be revised and updated as appropriate to maintain its currency. With the *Handbook* online, State Archives staff will cease to take such an active role in the examination process, although they will continue to be available for consultation.

Appendix 6: South Carolina Laws, Standards, and Guidelines Relating to Electronic Records

To ensure that records are properly created, maintained, and disposed, record keeping responsibilities of state and local government officials are well-defined in South Carolina's *Code of Laws*.

South Carolina Public Records Law and Electronic Records Management

Under South Carolina law

> A "public record" includes all books, papers, maps, photographs, cards, tapes, recordings, or other documentary materials regardless of physical form or characteristics prepared, owned, used, in the possession of, or retained by a public body." (Section 30-1-10 A)

The chief administrative officer of an agency or subdivision is the "legal custodian" of public records. He/she may appoint a records officer to act on his behalf. (Section 30-1-20).

The legal custodian of public records must protect them against deterioration, mutilation, theft, loss or destruction and make them available for easy use. (Section 30-1-70)

The head of each agency and the governing body of each subdivision and all legal custodians of public records must cooperate with the Department of Archives and History (DAH) and establish and maintain an active continuing program of records management. (Section 30-1-80)

Agencies and subdivisions must assist the DAH in conducting an inclusive records inventory and developing schedules mandating the retention of each series of records. (Section 30-1-90 A)

No records of long term or enduring value, including those generated and stored in electronic information systems or on magnetic, optical, film or other media may be destroyed or erased without an approved retention schedule. (Section 30-1-90 D)

Provided that authorized retention schedule procedures are followed, the legal custodian of public records is free from liability for his action in the destruction of public records. (Section 30-1-100 E)

The DAH has the authority to determine the medium in which archival records must be maintained or transferred to the Department, including those in electronic or optical disk systems. (Section 30-1-100 A)

The Department of Archives and History may examine all public records, including those otherwise restricted. (Section 30-1-90 A & C)

The Director of the Department of Archives and History may order the removal of records from facilities which do not meet Department regulations for records storage. (Section 30-1-70)

Other Relevant Statutes, Standards, and Guidelines

South Carolina Uniform Electronic Transactions Act

Enacted in 2004, the South Carolina Uniform Electronic Transactions Act (UETA) (South Carolina Code of Laws Section 26, Chapter 6) facilitates electronic commerce and electronic government services by legally placing electronic records and signatures on equal footing with their paper counterparts and officially repealing the 1998 South Carolina Electronic Commerce Act (South Carolina Code of Laws Section 26, Chapter 5). The law does not require the use of electronic records and signatures but allows for them where agreed upon by all involved parties. While technology neutral, the law

stipulates that all such records and signatures must remain trustworthy and accessible for as long as required.

South Carolina Enterprise Architecture, Uniform Electronic Transaction Act, South Carolina Standards for Electronic Signatures

In South Carolina's version of UETA, Section 26-6-190 states, in part:

> The South Carolina State Budget and Control Board shall adopt standards to coordinate, create, implement, and facilitate the use of common approaches and technical infrastructure, as appropriate to enhance the utilization of electronic records, electronic signatures, and security procedures by and for public entities of the State. Local political subdivisions may consent to be governed by these standards.

On February 28 2007, the South Carolina State Budget and Control Board, through its Architecture Oversight Committee, adopted *South Carolina Standards for Electronic Signatures*.

South Carolina Electronic Signatures Analysis and Implementation Guide

A task force of the South Carolina Architecture Oversight Committee is developing this guide to accompany the *South Carolina Standards for Electronic Signatures*. A link will be added to this document upon approval of the Architiecture Oversight Committee.

Appendix 7: Legal Issues Affecting Electronic Records Management

DISCLAIMER:
This is a summary tool. It is not intended to be a substitute for individualized legal advice. State agencies should consult legal counsel and the Office of the Attorney General for assistance with specific concerns or for advice.

There are a number of legal issues that affect electronic records management. This memorandum summarizes a few such issues, including: destruction of records/spoliation, discovery of electronic records, electronic records as evidence, privacy of e-mail, liability for records/information contained on a web site, personal jurisdiction via electronic records, and the Uniform Electronic Transactions Act.

I. Destruction of Records/Spoliation

A. Destruction in General

In *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (DC Cir 1993), a group of researchers and nonprofit organizations sought to prevent the deletion of e-mail records created during the Reagan administration, arguing that e-mail records should receive the same protection as paper-based records under the Federal Records Act (FRA). The DC Circuit agreed, holding that substantive e-mail communications are included in the FRA definition of "records" and so e-mail records, including transmittal information, should be stored. Often electronic records contain more information than their hard copy counterparts (such as multiple drafts in word processing). Machine-readable data contains original information that never existed in paper documents.

In *Public Citizen v. Carlin*, the Federal Court of Appeals overturned a lower court's holding that the federal government's General Record Schedule 20 (GRS 20) was invalid. GRS 20 governed the federal agencies' destruction and storage of certain electronic records. Specifically, the challenged portion of GRS 20 was the provision that authorized the disposal of word processing and electronic mail files that were copied to an agency record keeping system from a personal computer.

The lower court had held that GRS 20 exceeded the statutory authority because (1) it did not analyze the content of the records (it includes "program" records as well as "housekeeping" or administrative records); and (2) it did not set a specific time period for the retention of records before destruction (which is required by the statute). It also stated that hard copy records are not satisfactory replacements for electronic records and may impair the research value of the records, since hard copies cannot be searched, manipulated, and indexed in the same way as electronic records, and are not as complete as electronic records (such as information about revisions).

The Court of Appeals held that the statute required a record to be scheduled according to the physical attributes of the record rather than its content. In addition, GRS 20 only authorizes disposal of records after they are copied into an agency record keeping system. There is no risk that the information will be lost to future users, since a record must first be copied before it can be destroyed under GRS 20. GRS 20 does not authorize the disposal of electronic records per se. The National Archivist still has to assess the "administrative, legal, research, or other value" of a record before authorizing its disposal. The Court also held that GRS 20 did state a time for disposal of records, which was after they have been transferred

to a record keeping system. The Court of Appeals agreed with the lower court that electronic record keeping has advantages over paper record keeping, but acknowledges that not all agencies have established an electronic record keeping system and that the Archivist does not have to require every such agency to create an electronic record keeping system. Finally, the paper copies of electronic records will be complete, because GRS 20 required retention of hidden information or comments.

A defendant organization may seek to have a lawsuit dismissed for prejudice, if the plaintiff delayed in filing the lawsuit, and if before such filing the organization destroyed relevant records pursuant to its reasonable record retention policy. Minnesota courts are hesitant to impose sanctions for the destruction of documents prior to the initiation of litigation. *Capellupo v. FMC Corp.*, 126 FRD 545 (D MN 1989). Courts in other states do not hesitate to impose such sanctions, however. For example, in *Peskin v. Liberty Mutual Insurance Company* (530 A.2d 822 (1987)), Peskin filed a claim for insurance coverage 9 1/2 years after a fire. Liberty Mutual no longer possessed all the records necessary to establish the parameters of coverage. The records were destroyed by Liberty Mutual pursuant to its records destruction schedule before it received notice of the fire. The court remanded the case to determine whether Liberty Mutual's record retention policies comported with industry standards of practice and were otherwise reasonable.

The duty to preserve evidence starts when the litigant knows, or reasonably should know, that information is relevant in an action or reasonably calculated to lead to discovery of admissible evidence, is reasonably likely to be requested during discovery, and/or is subject of pending discovery request. (See *Souza v. Fred Carries Contracts, Inc.*, 955 P2d 3 (AZ App Div 2 1997) and *Fayemi v. Hambrecht and Quist, Inc.*, 174 FRD 319 (SDNY 1997)). For example, according to *Hunter v. Ark Restaurants Corp.*, 3 F. Supp 2d 9 (DDC 1998), a court can dismiss a case for destruction of evidence when the litigant is on notice that documents are relevant to potential litigation and destroys such documents, depriving the party of the opportunity to present critical evidence on key claims. The obligation to preserve evidence even arises prior to the filing of a complaint where a party is on notice that litigation is likely to be commenced. *Capellupo v. FMC Corp.*, 126 FRD at 550; *Alliance to End Repression v. Rochford*, 75 FRD 438 (ND IL 1976). If, however, there is no hint of litigation nor any other reason to retain certain documents, then a litigant's destruction of such documents does not warrant sanction or dismissal of the claim.

Each state has its own rules regarding destruction of evidence. For example, New York has a high standard for spoliation of evidence. Under its "Spoliator Beware" standard, the negligent, non-willful destruction of crucial and dispositive evidence in the sole possession of a party could bring severe sanctions of dismissal or summary judgment against the destroying party (even if the evidence was destroyed before a lawsuit was commenced). When a party alters, loses, or destroys key evidence before it can be examined by the other party's expert, the court has discretion as to sanctions. See *Conderman v. Rochester Gas & Electric Corp.*, 687 NYS2d 213 (Supp 1998). In *Conderman*, there was an accident caused by certain telephone poles falling on a car. The defendant's risk management department sent an experienced team of claims personnel to the accident site, and they did not mark, identify, preserve or test the poles. The poles were thereafter destroyed, and the plaintiff claimed spoliation of evidence. The court held that New York has a strong public policy regarding the maintenance of key evidence in connection with a lawsuit. In this case, the immediate dispatch of experienced claims personnel showed that the defendant had a high degree of awareness of the likelihood of possible litigation, and supports a finding that crucial evidence was negligently destroyed.

A majority of states do not recognize a separate tort of spoliation of evidence, but limit

the remedies for spoliation to the case at hand (such as Arizona in *Souza v. Fred Carries Contracts, Inc.*, 955 P2d 3 (AZ App Div 2, 1997); and Texas in *Trevino v. Ortega*, 969 SW2d 950 (TX 1998). Courts in these states hold that spoliation does not give rise to independent damages, and is better remedied within the lawsuit affected by the spoliation. Spoliation is an evidentiary concept, not a separate cause of action; the destruction only becomes relevant when someone believes that those destroyed items are instrumental to success in a lawsuit. A minority of states, however, do recognize a separate tort of spoliation of evidence (California, Florida, New Jersey, New Mexico and Ohio).

B. Destruction After Commencement of Lawsuit

Once an organization knows, or has reason to know, of the relevance of documents or information, it has an affirmative duty to preserve such information. If an organization destroys or fails to retain documents or information which it knows, or has reason to know, will be relevant in a lawsuit, it may face sanctions (at the discretion of the Court) for spoliation of evidence ranging from fines and penalties to entry of a judgment against it. See *Shepherd v. American Broadcasting Companies*, 151 FRD 179 (DDC 1992).

In determining whether a court should exercise its authority to impose sanctions for spoliation, a threshold question is whether a party had any obligation to preserve the evidence. Sanctions may be imposed on a litigant who is on notice that documents and information in its possession are relevant to litigation, or potential litigation, or are reasonably calculated to lead to the discovery of admissible evidence, and who destroys such documents and information. While a litigant is under no duty to keep or retain every document in its possession once a complaint is filed, it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably likely to be requested during discovery, and/or is the subject of a pending request. *Wm. T. Thompson Co. v. General Nutrition Corp.*, 593 F. Supp. 1443 (CD Cal 1984). Thus, no duty to preserve arises unless the party possessing the evidence has notice of its relevance. *Danna v. New York Telephone Co.*, 752 F. Supp. 594 (SDNY 1990). Of course, a party is on notice once it has received a discovery request. Beyond that, the complaint itself may alert a party that certain information is relevant and likely to be sought in discovery. *Computer Associates International, Inc. v. American Fundware, Inc.*, 133 FRD 166 (D CO 1990); *Teletron Inc. v. Overhead Door Corp.*, 116 FRD 107 (SD FA 1987).

For example, in *Applied Telematics, Inc. v. Sprint Communications* (1996 US Dist Lexis 14053), Sprint failed to preserve backup tapes of a computer system that routes telephone calls after receiving a request for information in connection with a patent infringement lawsuit commenced by Applied Telematics. Applied Telematics argued that Sprint knew that such information was relevant when it received the request for information. Sprint responded that, pursuant to its normal operating procedures, the computer system is backed up and saved, replacing the prior week's backup. As a result, after one week the historical information is unavailable from the computer system.

The court found that Sprint did know, or should have known, that the backup files were relevant, and failed to take steps to prevent the routine deletion of the backup files. The fact that Applied Telematics failed to ask Sprint to save the files does not relieve Sprint of its affirmative duty to do so. The court went on to find that Sprint did not destroy the backup files fraudulently or with the intent to prevent Applied Telematics from obtaining the evidence, and Applied Telematics did not suffer substantial prejudice from Sprint's actions. As a result, the court awarded Applied Telematics monetary sanctions for the destruction of evidence. The prejudice was not substantial, in part because Applied Telematics failed to pursue other means to obtain the information. The court held that it has discretion to

choose an appropriate sanction upon finding improper loss or destruction of evidence, based on the willfulness of the destructive act and the prejudice suffered by the requesting party. If the spoliation or destruction of evidence was intentional and indicates fraud and a desire to suppress the truth, rather than destruction that is a matter of routine with no fraudulent intent, a sanction that has a drastic result, such as entry of judgment, may be appropriate. See also *Shepherd v. American Broadcasting Companies,* 151 FRD 179 (DDC 1992).

Similarly, in *Turner v. Hudson Transit Lines, Inc.*, 142 FRD 68 (SDNY 1991), the court imposed sanctions on the defendant because it destroyed maintenance records of a bus and as a result was unable to produce them in a lawsuit regarding an injury that took place on the bus. The defendant maintained records for one year, as required by the Federal Highway Administration regulations, then destroyed the maintenance records pursuant to its documentation retention policies. The lawsuit was filed in October 1986, and the document request for maintenance records of the bus was made December 29, 1989. The defendant destroyed the documents in December 1989 and therefore could not produce them. The court held that, at least by the time the complaint was served, the defendant was on notice that maintenance records should be preserved. Even though it did not intentionally destroy evidence, its reckless conduct did result in loss of the records. The corporate managers were responsible for conveying this information to relevant employees. The defendant's management did not advise its employees of the obligation to maintain relevant documents while litigation was pending. It had an obligation to preserve the maintenance records and it failed to do so.

It is no defense for an organization to suggest that particular employees were not on notice. To hold otherwise would permit an organization to shield itself from discovery obligations by keeping its employees ignorant. See also *National Association of Radiation Survivors*, 115 FRD at 557; *Medical Billing, Inc. v. Medical Management Sciences, Inc. v. Reich*, 1996 WL 219657 (ND OH 1996).

Even though a party may have destroyed evidence prior to issuance of the discovery order and thus be unable to obey, sanctions may still be appropriate if the inability to produce the records was self-inflicted. See *In re Air Crash Disaster near Chicago, Illinois on May 25, 1979*, 90 FRD 613 (ND IL 1981). For example, in *Computer Association v. International v. Americal Fundware, Inc.*, 133 FRD (D CO 1990), the defendants destroyed a version of source code at issue after a copyright infringement lawsuit was filed. The defendant was sanctioned by the court because it had an obligation to preserve the code because of its knowledge of plaintiff's claims. See also *National Association of Radiation Survivors v. Turnage*, 115 FRD 543 (ND CA 1987); *ABC Home Health Services, Inc. v. International Business Machines Corp*, 158 FRD 180 (SD GA 1994); *General Environmental Science Corp. v. Horsfall*, 141 FRD 443 (ND OH 1992); *Hirsch v. General Motors Corp.*, 628 A2d 1108 (NJ Super 1993); *Lexis-Nexis v. Beer*, 41 F Supp2d 950 (D MN 1999); *Pepsi Cola Bottling Co. of Olean v. Cargill Inc., Archer-Daniels Midland Co.*, 1995 WL 783610 (D MN 1995).

C. Adverse Inference

If a party destroys evidence, a court may accept an inference that the evidence would be unfavorable to the position of the offending party. The concept of an adverse inference as a sanction for spoliation is based on two rationales: (1) remedial — where evidence is destroyed, the court should restore the prejudiced party to the same position with respect to its ability to prove its case that the court would have held if there had been no spoliation; or (2) punitive — to deter parties from destroying relevant evidence before it can be introduced at trial. If a party destroyed evidence, it may accept an inference that the evidence would be unfavorable to the position of such party. The rationale is based

on the observation that a party who has notice that evidence is relevant to litigation and who proceeds to destroy it is more likely to have been threatened by that evidence than is a party in the same position who does not destroy the evidence. See *Schmid v. Milwaukee Electric Tool Corp.*, 13 F3d 76 (3rd Cir 1994).

When an adverse inference is made, the party may have sanctions imposed, and/or the evidence can be admitted against it. The key considerations in determining whether such a sanction is appropriate are: (1) the degree of fault of the party who altered or destroyed the evidence; (2) the degree of prejudice suffered by the opposing party; and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party and, where the offending party is seriously at fault, will serve to deter such conduct by others in the future. See *Kronisch v. U.S.*, 150 F3d 112 (2nd Cir 1998); *Dillon v, Nissan Motor Co., Ltd.*, 986 F.2d 263 (8th Cir 1993); *SDI Operating Partnership LB v. Neuwirth*, 973 F.2d 652 (8th Cir 1992).

The state of mind of a party that destroys evidence is a major factor in determining whether an adverse inference is an appropriate sanction. If the party acted in bad faith or intended to prevent the use of the evidence in litigation, then an adverse inference is required; if the party acted willfully, it may be appropriate to draw an adverse inference. See *Alexander v. National Farmers Organization*, 687 F 2d 1173 (8th Cir 1982). Before an adverse inference is made, the party seeking the destroyed evidence must show that the destroyed evidence would have been otherwise unattainable by the party seeking such destroyed evidence. In order to remedy the evidentiary imbalance created by the destruction of evidence, an adverse inference may be appropriate even in the absence of a showing that the spoliator acted in bad faith. However, where the destruction was negligent rather than willful, special caution must be exercised to ensure that the adverse inference is commensurate with information that was reasonably likely to have been contained in the destroyed evidence.

For example, in *Brewer v. Quaker State Oil Refining Corp.*, 72 F3d 326 (3rd Cir 1995), the court stated that if the contents of a document are relevant to the issue in a case, the trier of fact generally may receive the fact that the document cannot be produced as evidence that the party who has prevented production did so out of well-founded fear that the contents would harm him or her if discovered. On the other hand, no unfavorable inference arises when circumstances indicate that the document or article in question has been lost or accidentally destroyed, or where failure to produce the document is otherwise accounted for. For example, when a company cannot produce an employee's personnel file because the employer's in-house attorney died of a terminal illness after taking possession of the file and the employer cannot find the file after continually looking for it.

D. Inefficient Record Keeping System: Unable to Locate Records

An organization may face liability if it creates a record keeping and indexing system that makes it difficult or costly to locate and produce documents on request. For example, in *Kozlowski v. Sears* (73 FRD 73, 1976), the plaintiff was burned when pajamas manufactured and marketed by the defendant ignited. The plaintiff asked for a record of all complaints and communications concerning personal injuries or death allegedly caused by the burning of children's nightwear manufactured or marketed by the defendant. The defendant refused to produce such documents, stating that there is no practical way for anyone to determine whether there are any such records, because it has a longstanding practice of indexing claims alphabetically by name of applicant, rather than by type of product. The court stated that the defendant may not excuse itself from compliance with the discovery request because it "utilizes a system of record keeping which conceals rather than discloses relevant records or makes it unduly difficult to identify or locate them, thus rendering the production

of the documents an excessively burdensome and costly expedition. To allow a defendant whose business generates massive records to frustrate discovery by creating an inadequate filing system, and then claiming undue burden, would defeat the purpose of the discovery rules." See also *Continental Illinois National Bank & Trust Company of Chicago v. Caton*, 136 FRD 682 (D KS 1991); *Baine v. General Motors Corp.*, 141 FRD 328 (MD AL 1991); *Fagan v. District of Columbia*, 136 FRD 5 (DDC 1991); *Control Data Corporation Securities Litigation*, 1988 WL 92085, Fed Sec L Rep 93,720 (D MN 1988); *Bowman v. Consolidated Rail Corp.*, 110 FRD 525 (ND Ind 1986); *US v. ACB Sales & Service, Inc.*, 95 FRD 316 (1982); *Dunn v. Midwestern Indemnity*, 99 FRD 191 (SD OH 1980); *Webb v. Westinghouse Electric Corp.*, 81 FRD 431 (ED PA 1978).

E. Requirement to Follow Internal Document Retention Policies

If a corporation has a documentation retention policy or other corporate policy that applies, it creates a standard that it is required to follow. For example, in *Gillispie v. Rank Video Services America*, (1997 US Dist LEXIS 13183), the court found that the defendant violated its own policy by not promoting the plaintiff, and this violation may constitute evidence of discrimination.

II. Discovery of Electronic Records

Today it is well established that computerized data and electronic records (as well as documentation of the computer system itself) are discoverable if relevant during discovery (the information-gathering process of a lawsuit). See FRCP 34(a); *Adams v. Dan River Mills Inc.*, 54 FRD 220 (WD VA 1972). Courts have stated that information which is stored, used, or transmitted in new forms should be available through discovery with the same openness as traditional forms. It would be dangerous if new techniques for using information became a hindrance to discovery in litigation. Specifically, a defendant's deleted files on its computer hard drive may be discoverable if they are still recoverable. See *Gates Rubber Co. v. Bando Chemical Indus. Ltd.*, 167 FRD 90 (D CO 1996); *Strausser v. Yalamachi*, 699 So2d 1142 (FA App 1996) *Anti-Monopoly, Inc. v. Hasbro, Inc.*, 1995 USLEXIS 6355 (SDNY 1995); *Seattle Audobon Society v. Lyons*, 871 F. Supp. 1291 (WD WA 1994); *Easley, McCaleb & Associates, Inc. v. Perry*, No. E-2663 (Ga. Super. Cit. July 13, 1994); *PHE, Inc. v. Department of Justice*, No. 96-2840 (PLF) (DDC 1991); *Pearl Brewing Co. v. Joseph Schlitz Brewing Co.*, 415 F. Supp 1122 (SD Tex 1976); *Greyhound Computer Corp., Inc. v. IBM*, (3 Computer L Serv Rep 138 D. MN 1971). When computerized data is produced, it must be in a form reasonably useable by the other party. If a party suspects that the other party is not producing all relevant information or has destroyed records, the party may request access to the other party's computer system, or visit the other party's site.

The proliferation of e-mail has changed discovery greatly. Many courts have upheld e-mail discovery requests, making e-mail messages fodder for legal action. Most e-mail systems can create a complex record of communication, capturing the exact text that users send and receive, as well as storing information regarding their transmission and receipt. Destroying e-mail is difficult. Even if a user deletes a message from his or her machine, most e-mail systems store messages on a centralized backup file indefinitely. It is relatively easy to retrieve deleted e-mails from most computer databases and these deleted e-mails are generally discoverable. See *In re Brand Name Prescription Drug Antitrust Litigation* (94-C-87, MDL 997 (ND IL 1995)).

Note, however, that the attorney-client privilege can extend to computer files. If legal counsel's advice or opinion was conveyed through electronic mail, then that message is privileged, except to the extent it contains information meant to be distributed to persons other than the corporate client. See *IBM v. Comdisco, Inc.*, (91-C-67-1992 Del Super LEXIS 67 March 11,

1992). As a result, e-mail communications received from legal counsel should not be forwarded to any party within the organization, unless such party has a need to know such information. In addition, security measures should be in place to ensure that other employees at an organization do not have access to each other's e-mail, including any e-mail communication from the organization's legal counsel.

Amendments to the Federal Rules of Civil Procedure effective December 1, 2006 make electronic records a routine element in litigation. Because of these changes, both businesses and public sector entities have more incentive to maintain their email files over a longer period of time. Premature destruction of email or failure to account for electronic records may now entail harsher penalties than in the past [see particularly FRCP 26(a) and FRCP 16(b)].

III. Electronic Records as Evidence

Computer-generated records cannot be admitted into evidence unless the proper foundation has been laid. For example, in *Illinois v. Bovio* (455 NE2d 829, 1983), the court ordered a new trial because the state prosecutor did not lay the proper foundation for admitting computer-generated bank records into evidence, which supported a necessary element of the charge of theft by deception. In Illinois, it must be shown that the computer equipment is standard, that the entries are made in the regular course of business at or reasonably near the time of the happening of the event recorded, and that the sources of information and the method and time of preparation are such as to indicate trustworthiness and justify admission. There was no testimony to show how transaction information was entered into, and processed through, the computer system which would verify the accuracy of the output. Systems which perform calculations must be scrutinized more thoroughly than systems which merely retrieve information. The state needed to show that the computer program was standard, unmodified, and operated according to its instructions.

Other states have more liberal rules regarding the admissibility of electronic records into evidence. For example, the California Uniform Electronic Evidence Act (Act) defines "electronic record" and "electronic records system" and provides a series of rules and presumptions relating to the admissibility of electronic records. The key to the Act is the presumption of integrity given to electronic records when it is established that (a) at all material times the computer system was operating properly or the fact that it was not operating properly did not affect the integrity of the electronic records; and that (b) there are no reasonable grounds to doubt the integrity of the electronic records system.

One way in which to admit electronic records into evidence in federal court is by defining them as "business records" under the Federal Rules of Civil Procedure, therefore excepting them from hearsay. The business records exception relies on trustworthiness and necessity. It consists of five elements: (1) the records must be kept in the ordinary course of business; (2) the particular record at issue must be one that is regularly kept; (3) the record must be made by, or from, information transmitted by a person with knowledge of the source; (4) the record must be made contemporaneously; and (5) the record must be accompanied by foundation testimony by a custodian of the record. All such elements must be met to be admissible. Critical to admissibility of computer records is the foundation testimony regarding the above requirements, including the reason that the message was prepared and sent. See *U.S. v. Catabran*, 836 F.2d 453 (9th Cir 1988); *Rosenberg v. Collins*. See also *Quality Auto Service v. Fiesta Lincoln-Mercury Dodge Inc.*, No. 04-96-00967-CV 1997 WL 563176 (TX App Sept 10, 1997); *U.S. v. Kim*, 595 F2d 755 (DC Cir 1979).

Electronic records and computer printouts of accounting and other bookkeeping records that are entered into the computer on a monthly basis are generally admissible in court as business records. See *Midfirst Bank SSB v. CW Haynes & Co.*, 893 F. Supp 1304 (DSC 1994); *U.S. v. Goodchild*, 25 F3d 55 (1st Cir 1994). Electronic records reveal more information than their paper counterparts, since they more easily show inconsistencies among documents, contain multiple drafts of documents, contain the history of a document (including who revised the document, in what manner, and when), may contain unprinted annotations, and show the names of documents and other filenames. Electronic data thought to be lost or erased is usually accessible. In addition, there are usually multiple drafts of documents and many different places within a network or computer they may be stored. Data is routinely backed up over and over, and exists in many different places and formats. Users are adverse to destroying data, people use a lower standard of care when writing e-mail, and computers routinely save many copies of documents in various ways. This makes it very expensive, time consuming, and burdensome to find and produce electronic records. In addition, if you do not produce the records, your adversary may gain access to your computer system.

The admissibility of e-mail is not so clear, however. Although e-mail is obtainable through discovery, there is no guarantee that it will be admissible in federal court. Courts are concerned about whether e-mail satisfies the "regular practice" of the exception, and the casual nature of the messages raises trustworthiness questions. See *Aviles v. McKenzie; Strauss v. Microsoft Corp.; Allen v. State; U.S. v. Kim* 595 F2d 755 (DC Cir 1979); *Plymouth Police Brotherhood v. Labor Relations Commission; Monotype Corporation PLC v. International Typeface Corporation*, 43 F.3d 443 (1994).

As of 1996, no federal court had applied the business records exception to e-mail messages. Since then, some courts have held it is admissible, while others have held that it does not meet the requirements of the business records exception in the Federal Rules of Evidence (Rule 803(6)). For example, in *Monotype Corporation PLC v. International Typeface Corporation*, 43 F.3d 443 (1994), the court excluded an e-mail transmission as evidence to support the defendant's defense. The defendant moved to admit an e-mail transmission under the business records exception to support its defense that it did not copy Monotype's typefaces. The court held that e-mail is far less of a systematic business activity than a monthly inventory printout or other computer-generated printout. E-mail is an ongoing electronic message and retrieval system, whereas an electronic inventory recording system is a regular, systematic function of a bookkeeper prepared in the course of business. See also *Michaels v. Michaels; Monotype Corporation PLC v. International Typeface Corporation*, 43 F.3d 443 (1994); *U.S. v. Catabran*, 836 F.2d 453 (9th Cir 1988); *U.S. v. Kim,* 595 F2d 755 (DC Cir 1979).

A survey of recent federal cases, however, shows that e-mail has found its way into the courtroom. For example, in *Knox v. State of Indiana*, 93 F3d 1327 (7th Cir 1996) e-mail messages in which a supervisor repeatedly asked an employee for sex were admissible in a harassment case. See also *Harley v. McCoach*, 928 F. Supp. 533 (ED PA 1996); *Wesley College v. Pitts*, 874 F.Supp 375 (D DE 1997).

IV. Privacy of E-Mail

An employee has no reasonable expectation of privacy in e-mail communications voluntarily made over the company e-mail system to another company employee, notwithstanding assurances that such communications would not be intercepted by management. For example, in *Smythe v. The Pillsbury Company* (914 FSupp 97, 1996), the court held that Smythe could be fired for communications made to his supervisor which were forwarded to Pillsbury management. The court found that such a firing does not violate Pennsylvania public policy,

and that monitoring and interception of the contents of e-mail communications made over the company e-mail system by an employer does not invade an employee's privacy interests.

See also *Bourke v. Nissan Motor Corp.*, No. B068705 (CA Ct App, July 26, 1993), which stated that employees had no reasonable expectation of privacy in their work place e-mail when (a) they were aware for some time prior to being terminated that their e-mail was read by the company; and (b) they signed a statement agreeing to restrict their use of company-owned hardware and software to company business.

V. Liability for Records/Information Contained on Web Site

A. Copyright

Web sites have been held liable for intellectual property infringement and other harms caused by their users. A single bad user could cause liability ranging into the millions of dollars. The potential legal risks inherent in owning and maintaining a web site are copyright infringement (direct, contributory, or vicarious) and defamation. Web sites planning to permit users to exchange content should implement a number of techniques to manage their potential risk. In addition, a president, officer, and shareholder in a defendant corporation may be personally liable for the activities of the company, since he or she is active in the day to day operations of the company. See *Religious Technology Center v. Netcom On-Line Comm*, 907 F. Supp 1361 (ND Cal 1995).

For example, in *Comedy III Productions, Inc. et al v. Class Publications, Inc. et al* (1996 US Dist LEXIS 5710 April 30, 1996), the defendant violated plaintiff's trademarks in the Three Stooges by selling unauthorized products on its Internet web site. In addition, Playboy Enterprises has initiated a number of lawsuits against web sites that post its copyrighted pictures, or that allow a subscriber to the web site to upload such pictures to the web site. For example, in *Playboy Enterprises, Inc. v. George Frena*, 839 F Supp 1552 (1993), the defendant operated a subscription computer bulletin board service, which distributed unauthorized copies of plaintiff's photographs. On the web site, subscribers could log on and browse and download pictures and store them on their personal computers. In addition, subscribers could upload material to the web site so that all other subscribers could view the material. The defendant admitted that the pictures were displayed on his web site, but claimed that he did not place them there; they were uploaded by a subscriber. The defendant did not know about the pictures until he was served complaint papers, at which time he removed the photographs and began monitoring the web site to prevent additional photographs from being uploaded. The court held that the defendant is responsible for material that is on his web site and infringes on another's copyright, even if the defendant did not place the material on the web site and did not have knowledge that such material so infringed. See also *Playboy Enterprises, Inc. v. Webbworld, Inc.*, 991 F Supp 543 (ND Tex 1997); *Christopher Scanlon v. Gil Kessler et al*, No 97 Civ 1140, 1998 US Dist Lexis 10201 (SDNY July 10, 1998). Further, an operator of a computer bulletin board service may become liable for copyright infringement if it takes affirmative steps to cause copies to be made. For example, if a bulletin board service encourages people to upload documents, and it screens all documents and moves them to the appropriate generally available files, it may be held liable for things posted on its web site by others. See *Playboy Enterprises Inc v. Russ Hardenburgh, Inc.*, 982 F. Supp 503 (ND Ohio 1997).

The Digital Millennium Copyright Act (("DMCA") (17 U.S.C§ 1201 et seq; passed by Congress in 1998) makes changes in United States copyright law to address our current digitally networked environment. The DMCA provides for a limitation on "online service providers" liability for monetary damages and injunctive relief with respect to copyright infringement

in certain circumstances. It adds a safe harbor to the current United States copyright law. Online service providers are defined as those entities that link users to the internet and facilitate the transmission of digital data that is translated into another party's copyrighted work. The DMCA provides a safe harbor from liability for online service providers if their online system complies with the procedures and certain requirements set forth in the DMCA, which include the following: (1) the organization meets the definition of an online service provider, (2) the organization engaged in covered activities, and (3) the organization meets the conditions in the DMCA for material, parties to transmission, and procedures. To qualify for the limitation, the material that is transmitted online must be made available by someone other than the online service provider, and the online service provider cannot modify the material. In addition, the online service provider cannot have actual knowledge of any copyright infringement and must cooperate with the processes to disable access and limit harm to the copyright owner in the event of infringement. The safe harbor does not apply to copyrighted material the online service provider may place online itself or through independent contractors, such as on its home page; such material is subject to a traditional copyright analysis under current law.

B. Defamation

In general, courts have been reluctant to hold web site owners liable to defamatory statements made by others on its web site, such as statements made in chat rooms and other interactive medium. The Communications Decency Act, passed in 1996, states that no provider or user of an interactive computer service shall be treated as a publisher or speaker of any information provided by another information content provider. To date, courts have treated this language as a nearly complete bar against liability for users' defamatory postings. The safe harbor only applies to information provided by another organization or person, however, and does not apply to information put on the web site by the defendant itself.

As a result, in general computer bulletin board services are not liable when people post things without authorization and the web site operator does not create or control the content of the information available to its subscribers, but merely provides access to the internet. In *Cubby, Inc. v. Compuserve, Inc.*, No. 90 Civ 6571 (SDNY 1991). Cubby was suing Compuserve for libel, unfair competition, and business disparagement based on allegedly defamatory statements made in a publication included in a computerized database. The court found that Compuserve had no opportunity to review the allegedly defamatory information before it was uploaded into computer banks, from which it is immediately available to subscribers. In addition, Compuserve received no part of the fees charged for access to the relevant database; it has just one main subscription fee. The court found that Compuserve acted as a distributor, and not a publisher, of the statement and cannot be held liable for the statement because it did not know and had no reason to know of the statements. Once Compuserve decides to carry a publication, it has little or no editorial control over that publication's contents. In this situation, Compuserve is like a bookstore, library, or news stand.

On the other hand, an operator may become liable if it takes affirmative steps to cause copies to be made. For example, if a bulletin board service encourages people to upload documents, and it screens all documents and moves them to the appropriate generally available files, it may be considered to have "republished" the material. One who repeats or otherwise republishes defamatory matter is liable as if he or she had originally published it. But, vendors and distributors of such matter are not liable unless they knew or had reason to know about it. In *Stratton Oakmont, Inc. v. Prodigy Services Company*, Supreme

Court, State of New York Index No. 31063/94, Stratton is suing Prodigy for libel based on allegedly defamatory statements made in on Prodigy's "Money Talk" computer bulletin board. Prodigy held itself out as an online service that exercised editorial control over the content of messages posted on its computer bulletin boards, thereby expressly differentiating itself from its competition, and expressly likening itself to a newspaper. It has a series of "content guidelines" and enforced them through an automatic software screening program. Prodigy actively utilized technology and manpower to delete notes from its computer bulletin boards on the basis of offensiveness and bad taste; Prodigy is clearly making decisions as to content and such decisions constitute editorial control. As a result, Prodigy is a publisher rather than a distributor and can be sued for libel. Prodigy's conscious choice, to gain the benefits of editorial control, has opened it up to a greater liability than other computer networks that make no such choice (such as Compuserve, above).

C. Risk Management

The following are suggestions for a web site to take to minimize its risk regarding potential copyright infringement and defamation liability:

1. Do not actively monitor the web site. Active monitoring of the web site will give the web site actual or putative knowledge of user conduct and content. Thus it creates the possibility that a web site will be liable for all user harms except those preempted by the safe harbor described above.

2. Consider empowering independent contractors to monitor your site and give them the authority necessary to resolve problems.

3. Respond to complaints promptly.

4. Review your user agreement(s). Provisions enabling the web site to blacklist subscribers or edit content on subjective or arbitrary standards provide strong evidence of the web site's right and ability to control its users and their content. User agreements should only prohibit users from engaging in conduct that is illegal or tortuous.

5. All employees who interact with the web site can take legally significant actions that could undermine a risk management strategy; thus the web site's risk management strategy should be explained to all employees, and employees responsible for dealing with web site problems should be given special training on how to implement strategies.

VI. Personal Jurisdiction via Electronic Records

The minimum contacts required for personal jurisdiction in another state can be electronic. As a result, an organization that posts advertisements on the Internet through its web site may be subject to jurisdiction in all states in which such information can be accessed. For example, in *Inset Systems Inc. v. Instruction Set, Inc.,* (937 F. Supp. 161, 1996), the court found that ISI was subject to Connecticut jurisdiction because it had a toll-free telephone number and an Internet web site on which it posted advertisements. There are at least 10,000 internet-connected computer users in Connecticut, all of which could access ISI's advertisements again and again.

In addition, a person who conducts business via electronic mail with a person in another state is subject to jurisdiction of the courts in such state. In *Hall v. Laronde* (666 CA Rptr 2d 399, 1997), a California court held that a person living and working in New York may be sued in California when he negotiated the purchase, and of software modification from a California resident via electronic mail and the telephone, even though the California resident reached out to the defendant first. The defendant worked with the California resident through a period of

time, and made continuing royalty payments, thus creating a continuing obligation between himself and the California resident.

VII. Uniform Electronic Transactions Act

The purpose of the Uniform Electronic Transactions Act (UETA) is to develop an act relating to the use of electronic communications and records in contractual transactions. The UETA governs electronic records and signatures relating to a transaction, defined as limited to business, commercial and governmental affairs. It is intended to be consistent with the Uniform Commercial Code, but not duplicative of it. As a result, the UETA is procedural and affects the underlying substantive law of a given transaction only if absolutely necessary in light of the differences in media used. Whether a record is attributed to a person, and whether an electronic signature has any effect, is left to other substantive law.

The UETA expressly validates electronic records, signatures, and contracts. It affects the medium in which information, records, and signatures may be presented under current legal requirements. It provides for the use of electronic records and information for retention purposes, providing certainty in an area with great potential in cost savings and efficiency. The UETA makes clear that the actions of machines programmed and used by people will bind the user of the machine, regardless of whether a human was involved in a particular transaction. It also specifies the standards for sending and receiving electronic records. South Carolina's version of UETA directs the South Carolina State Budget and Control Board to adopt standards for electronic records, electronic signatures, and security procedures. South Carolina's *Standards for Electronic Signatures* were adopted on February 28, 2007. Certain legal rules requiring certain writing and signatures under law are not affected by the UETA (such as wills, etc). It applies only to transactions between parties who have agreed to conduct transactions electronically; it is intended to facilitate the use of electronic means, not require the use of electronic records and signatures.

The requirements for electronic transactions are as follows:

1. Confidentiality: the contents of messages or substance of transactions must be kept secret to unauthorized parties.
2. Access control/confidentiality: the information is only available to authorized parties; the access to information is controlled, and distribution or disclosure of the records is restricted.
3. Chain of custody: the authentication of stored electronic records (this strengthens the credibility and privacy of records).
4. Message integrity: the message is not tampered with; it is accurate.

The UETA provides that a record or signature may not be denied legal effect or enforceability solely because it is in electronic form. The medium in which a record, signature, or contract is created, presented, or retained does not affect its legal significance. It also provides that electronic records and signatures do satisfy legal requirements for writings and signatures, provided the parties have the ability to retain (print or download) the information for later review. An electronic record or electronic signature is attributable to a person if it was the act of the person. It may be proven by showing the efficacy of any security procedures applied to determine the person to whom the electronic record or signature was attributable.

The UETA also governs the retention of electronic records. It states that if a law requires certain records (including checks) to be retained, that requirement is met by retaining an electronic record that accurately reflects the information and remains accessible for later reference. The requirement of continuing accessibility addresses the issue of technology obsolescence and the

need to update and migrate information to developing systems. The UETA would permit parties to convert original written records to electronic records for retention, and states that electronic records can be considered originals so long as the accuracy and accessibility requirements are met. The concern focuses on the integrity of the information and not with its originality. So long as there exists reliable assurance that the electronic record accurately reproduces the information, the electronic records and paper-based records are functionally equivalent.

The UETA provides that, in a legal proceeding, evidence of an electronic record or signature may not be excluded from evidence because it is an electronic record or signature, or it is not an original. Admissibility of evidence depends upon the substance of the information rather than the media in which the information is presented.

The UETA contains provisions specific to electronic records by government agencies. It authorizes (but does not require) state agencies to use electronic records and signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and signatures. It gives an option to leave the decisions to each government agency or to assign that duty to a state officer. It also authorizes the destruction of written records after conversion to electronic form. In addition, the UETA broadly authorizes (but does not require) state agencies to send and receive electronic records and signatures in dealing with non-governmental persons. The UETA requires government agencies or state officers to take account of consistency in applications and interoperability among state agencies to the extent practicable when promulgating standards. For purposes of check retention statutes, the same electronic record of the check is covered by the UETA, so that retention of an electronic image/record of a check will satisfy such retention statutes so long as certain requirements are fulfilled.