Section 9:
Criteria for Trustworthy Information Systems

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 falls under the Minnesota Government Data Practices Act?
- What data is of permanent/historical value to you and/or to others?

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.

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 Minnesota 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.

QUESTIONS TO ASK

- What is the system's unique identifier and/or common name?
- 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?
- Were design reviews and system tests 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?

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)

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

Did You Know:

☑ "Agencies shall take reasonable measures to ensure that only agency authorized computer equipment is installed on or connected to state systems and that only approved software is installed or executed on state computer resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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.

- 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.

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

5. record formats and codes

6. routine performance of system back-ups. Each back-up should be documented with back-ups 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.

   - ➥ 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

   Did You Know:
   - ☑ "The agency head shall ensure that agency employees understand the importance of security measures and their role in sharing the responsibility for the security and integrity of state computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   - ☑ "Agencies shall make a copy of the state Security Policy available to each agency employee and shall make all employees, contractors, and information users aware of

their responsibilities under the state Security Policy and the agency security plan." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "The agency head shall ensure that each agency employee is aware that violation of the principles of the state Security Policy or the agency security plan could be cause for disciplinary action or termination from employment." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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.

QUESTIONS TO ASK

- 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?
- 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?
- Is there a list of all internal and external user groups and the types of data created and/or accessed?
- Have all positions been reviewed with respect to appropriate security levels?
- What are the procedures for the destruction of controlled-access hard copies?
- How is information purged from the system?
- How is reuse of hardware, software, and storage media prevented?

2A. User Identification / Authorization

1. User identification and access procedures should be established and documented. Users should be authenticated prior to being granted access.

   Did You Know:

   ☑ "Agencies shall limit access to computerized information resources and computer systems to authorized users." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "Agencies shall identify and control each point of access to computerized information or computer systems by an appropriate security method." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "Agencies shall establish and use appropriate authentication methods to ensure each user is identified prior to granting access to computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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.

Did You Know:

☑ "Authorized users of computerized information resources shall not disclose their means of authentication." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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.

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.

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.

   Did You Know:

   ☑ "Each agency that chooses to use digital signature technology must establish a digital signature implementation and use policy." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "An individual must protect and not disclose or make available his or her digital signature private key or password to other persons, including fellow state employees, managers, and supervisors." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

   ☑ "When conducting State business, an employee must only use a digital signature key pair and certificate purchased with state funds. Employees must not use a State digital signature key pair for personal business." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

- ☑ "The agency must revoke the ex officio digital signature key pair whenever there is a change in the person occupying the office." (Minnesota Department of Administration, Office of Technology, *Minnesota State Agency Digital Signature Implementation and Use Standard.* IRM Standard 18, Version 1. 19 November 1999.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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.

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. Failsafes 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.

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), call backs, 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

Did You Know:

- ☑ "Organizations conducting business over the Internet need robust security controls to ensure data integrity, data confidentiality, and system availability. Data integrity controls help protect the accuracy and completeness of data, both in storage and while in transit. Confidentiality controls help ensure that sensitive data, such as credit card numbers, cannot be seen by unauthorized individuals. Finally, system availability controls help minimize the amount of time when citizens cannot use the system to conduct business." (Office of the Legislative Auditor, *Financial-Related Audit: Department of Public Safety, Web-Based Motor Vehicle Registration Renewal System as of April 2001*. August 2001, Report No. 01-43.) [http:// www.auditor.leg.state.mn.us/]

- ☑ "It is a sad reality that unscrupulous individuals discover new discover new security exploits daily and use that knowledge to penetrate organizations with many layers of preventative defenses. This inherent security administration problem is why every organization must vigilantly monitor its systems for signs of attack. Since time is of the essence when under attack, every organization must also have decisive incident response procedures. Those that do not may fail to discover that they are completely unsecured until extensive damage has been done." (Office of the Legislative Auditor, *Financial-Related Audit: Department of Public Safety, Web-Based Motor Vehicle Registration Renewal System as of April 2001*. August 2001, Report No. 01-43.) [http:// www.auditor.leg.state.mn.us/]

- ☑ "Agencies shall take appropriate preventative actions to protect their computer information from corruption by viruses." (Minnesota Department of Administration, Office of Technology, *Computerized Information*

Resources Security Standards for State Agencies. IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

- ☑ "Agencies shall monitor and evaluate, on an ongoing basis, the effectiveness of security tools and virus protection being used within their agency. Security tools and virus protection systems which are not found to be effective shall be updated in a timely manner." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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?
- What mechanisms are available to designate which activities are audited? Who can do this?
- How are audit logs protected?

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

Did You Know:

☑ "The agency head shall ensure that users are aware that their use of computerized information resources is traceable." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Agencies shall ensure that computer access points to systems connected to the state network require and access control process that can be audited." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Where appropriate, agencies shall log access to data in such a way as to permit an agency to audit its access to computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16,

Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ Users must be supplied with the Tennessen Warning when collecting confidential, private data by any means. (Minnesota. *Chapter 13 (Government Data Practices, 13.04, subdivision 2). Statutes*. 1998.) [http://www.revisor.leg.state.mn.us/stats/13/]

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)

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:

☑ "Agencies shall ensure the backup, transport, storage, and recovery of their computerized information resources." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

☑ "Agency heads shall ensure that security policies are included in their Disaster Recovery Plans." (Minnesota Department of Administration, Office of Technology, *Computerized Information Resources Security Standards for State Agencies.* IRM Standard 16, Version 1. June 1998.) [http://www.ot.state.mn.us/ot_files/handbook/standard/standard.html]

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 Minnesota Department of Administration, InterTechnologies Group for assistance with incident-handling procedures and support.
    a. Information regarding the Minnesota Computer Emergency Response Team (MNCert) is available from James Johnson (651.296.6364; james.johnson@state.mn.us) and Arik Nelson (651-296-6361).

3. Related resources include :
    a. CERT Coordination Center [http://www.cert.org]

4C. Disaster recovery plans.

1. Hazards include:
    a. fire and/or explosion
    b. water or flood
    c. wind or tornado
    d. lightening
    e. power outage
    f. rodents
    g. insects
    h. human error
    i. violence and/or terrorism

2. Government agencies should contact the Minnesota Department of Administration, InterTechnologies Group, Business Continuation Management (BCM) Unit.
    a. The BCM can assist with:
        1. business impact analysis
        2. recovery strategy development
        3. plan development
        4. training
        5. plan test coordination
        6. plan maintenance
    b. Information regarding the BCM and ts services is available at: [http://www.mainserver.state.mn.us/bcm/]

3. Related resources include:
    a. Minnesota State Archives' record storage and disaster preparedness guidelines available at: [http://www.mnhs.org/preserve/records/recser.html#guides]

    b. Federal Emergency Management Agency (FEMA), emergency response and recovery guidelines available at: [http://www.fema.gov/r-n-r/ers_wl.htm#]

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?

Did You Know:

☑ The *Minnesota Recordkeeping Metadata Standard* is administered by the Minnesota Department of Administration, Office of Technology, as IRM Standard 20. The standard is geared to Minnesota government entities at any level of government. It includes both mandatory and optional elements, and may be applied at either the record or record series level. The standard is referenced in the *Minnesota Enterprise Technical Architecture* under Chapter 4, "Data and Records Management Architecture." [http://www.ot.state.mn.us]. For a complete discussion of the standard's purpose, structure, and requirements, see [http://www.mnhs.org/preserve/records/metadatastandard.html].

5A. The Minnesota Recordkeeping Metadata Standard 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

- 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?

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.

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.

Did You Know:
☑ Under the Minnesota standard, modified records are considered new records and are thus assigned new identifiers.

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 authenticated, 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.