



**STATE OF ALASKA**

**BUILDING A TRUSTWORTHY  
INFORMATION  
SYSTEM**

**January 2009**



**Department of Education & Early Development  
Division of Libraries, Archives & Museums  
Archives & Records Management Program  
POB 110525  
141 Willoughby Avenue  
Juneau, Alaska 99811-0525  
[Records Management Homepage](#)**

# TABLE OF CONTENTS

Forward . . . . .	Page ii
What's In It For Me? . . . . .	Page 3
Purpose of This Handbook . . . . .	Pages 4 - 5
What is a Trustworthy Information System? . . . . .	Page 6
What is the Process For Establishing Trustworthiness? . . . . .	Page 7
Who Should Participate? . . . . .	Page 8
Meta Data & Documentation . . . . .	Pages 9 - 10
How Important is Your Information? . . . . .	Pages 11 - 12
How Do You Apply the <i>TIS</i> Design Criteria? . . . . .	Pages 13 -14
What are the Design Criteria for a <i>TIS</i> . . . . .	Page 15
Design Criteria Group 1, System Documentation . . . . .	Pages 16 - 19
Design Criteria Group 2, Security Plan . . . . .	Pages 20 - 25
Design Criteria Group 3, Audit Trails . . . . .	Pages 26 - 27
Design Criteria Group 4, Record Metadata . . . . .	Pages 28 - 29
Glossary . . . . .	Pages 30 - 46
Bibliography & References . . . . .	Pages 47 - 57

# Forward

We are experiencing a world-wide fundamental paradigm shift: from media-centric records, where management is based on observable physical location controlled by humans; to the new era of digital information with content-centric records, where the management process is based on invisible logical location controlled by computers. [Courtesy: Robert F. Williams, Cohasset Associates]

*Building a Trustworthy Information System* is intended to span the human-machine information management gap and is modeled upon work previously completed by the Minnesota Historical Society's Trustworthy Information Systems Project, funded by a grant from the National Historical Publications & Records Commission. The Minnesota State Archives authorized the Alaska State Archives to incorporate certain portions of their *Handbook* into this monograph.

This publication also incorporates discrete elements of the *Systems Development Life Cycle Checklist* developed by the National Archives & Records Administration. The *Checklist* addresses questions relevant to information system life cycle processes to ensure that all functional and user requirements are met; and, that agency strategic goals and objectives are accomplished.

*Building a Trustworthy Information System* serves as an analytical tool and is not intended to substitute for agency-specific legal advice from the Attorney General's Office or independent counsel. Staff should also consult the Electronic Practices Committee prior to implementing a new system to determine whether any new electronic records standards have been approved.

D. Dawson, CRM  
State Records Manager  
[dean.dawson@alaska.gov](mailto:dean.dawson@alaska.gov)



# WHAT'S IN IT FOR ME?

So...why is *Building a Trustworthy Information System (TIS)* important? Information system developers, policy makers, and current/future system users must be confident that their information stores contain reliable, authentic and accessible information and records for the complete information life cycle of the record.

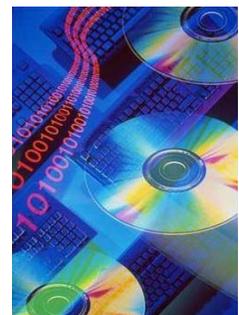
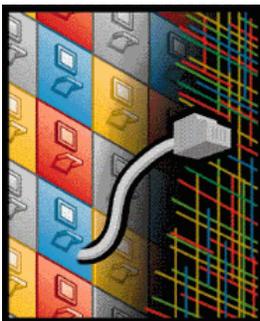
This *Handbook* provides information to:

- Understand why trustworthy information systems are important
- Apply statutory and legal mandates and policies to information management
- Document defensible level of government accountability
- Determine the strategic importance of your agency records and information
- Establish how much record keeping documentation or evidence is adequate

Government records and information are important because they:

- Facilitate government business
- Demonstrate government accountability
- Serve as evidence of government activity for current/future users of government information

Did you know that ninety-five percent of all current information is electronic? Accordingly, State of Alaska digital records must be reliable and authentic, just as paper records have been over the years. Since we cannot touch, feel, hold and examine electronic records in any intelligible way without the assistance of functional hardware and software, this *Handbook* provides design criteria for consideration to ensure that government information systems are trustworthy.



# PURPOSE OF THIS HANDBOOK

The purpose of this *Handbook* is assist agency staff in evaluating the technical and non-technical aspects of information systems in order to determine their trustworthiness. The *Handbook* presents information system design criteria so that staff can administer its information assets in accordance with the State Records Act (AS 40.21.)

The *Handbook* answers the following questions:

- What is meant by a trustworthy system?
- What should be considered for establishing trustworthiness?
- Who should participate and provide input?
- What is record metadata and why is it so important?
- How important is your information?
- Which *Trustworthy Information System* design criteria should you consider?

Further, the *Handbook* provides additional background and useful information including:

- A *Glossary* of relevant terms
- Pertinent laws and policies
- *Systems Development Life Cycle Checklists*

Information systems include *data*, *information* and *records*.

***Data*** simply assert facts but provide no context for those facts. Data can be discrete elements in a field in a database or the dynamic components of a web page.

***Information*** has meaning to us based on the context of its creation and use. Information can be a customized report from a database or the results of a database query.

***Records***, on the other hand, are accessed, understood and retained as evidence of a particular situation or event. These may include the minutes from a meeting or all the data captured as evidence of an electronic commerce transaction. Please refer to the *Appendix* for the statutory definition of "Record."

# PURPOSE OF THIS HANDBOOK

The evidentiary value of records is seriously undermined if the records are not placed and maintained in their appropriate administrative context. Thus, information management is different from data management since it requires the creation and maintenance of context. Records management, in addition to managing context, also ensures that the data or information have evidentiary value.

Though all of the elements of a record may exist within a single computer file, they may also be distributed across the enterprise. The integrity of these elements and the links between them are much more important than where they physically reside.

Although it is never too late to analyze system trustworthiness, it is optimal to do so during early system development. It is during the analysis phase of system development, prior to expenditure of considerable resources on design, that *TIS* design criteria can best be weighed and implemented. However, the *Handbook* is useful at any point during the system development life cycle.

You can also use the *Handbook* to examine the trustworthiness of your existing legacy systems, documenting what you presently have and how well the system is set up to meet various requirements. Due to the dynamic environment of information systems—hardware, software, platforms, architecture, communication methods—trustworthiness should be revisited at regular intervals.

The *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 criteria that your agency can apply, practically and efficiently.

# WHAT IS A TRUSTWORTHY INFORMATION SYSTEM?

Trustworthiness refers to an information system's integrity and its ability to produce reliable and authentic information and records. Trustworthy denotes ability, confidence and accountability. A reliable record refers to its authority which is established at its creation. Authentic records remain reliable throughout their life cycle--from birth to death or preservation.

The State of Alaska enterprise creates a plethora of information and records in a variety of methods and formats for numerous reasons. Records are created and received as agencies conduct the State's business and must be retained for administrative, legal, financial and historical purposes. Many of these electronic records must remain readable, interoperable, and compatible with assistive technology for extremely long periods of time. A few records have enduring historical value and warrant permanent preservation.



**Accountability.** The State's information, records and processes must be accountable. Statutes, regulations, policies, procedures, rules and other directives demand accountable systems to prove that actions are performed in accordance with prescribed standards. Records also document the history of Alaska; they contain valuable information about our citizens and the social, economic, political and natural environments in which we live.

Government accountability needs to be considered when information systems are developed. As subject matter experts and technologists make these systems accountable, it is critical to establish and create fully authorized procedural documentation and adequately describe system information.

Alaska State Government needs trustworthy information systems to ensure accountability to its citizens.

# WHAT IS THE PROCESS FOR ESTABLISHING TRUSTWORTHINESS?

Establishing the trustworthiness of an information system typically takes several steps and requires the collaboration of individuals with specialized knowledge, skills and abilities. This *Handbook* describes the process and guides the reader throughout the examination. The proper establishment of the trustworthiness of an information system depends on the completeness of the examination process.



**Step A:** Assemble Evaluation Team (Page 8, Who Should Participate?)

**Step B:** Cornerstone of a *Trustworthy Information System*  
(Pages 9 & 10, Metadata & Documentation)

**Step C:** Determine Value of your Data  
(Pages 11 & 12, How Important is Your Information?)

**Step D:** Application of Design Criteria (Page 13)

**Step E:** What are the Design Criteria for a *Trustworthy Information System*?  
(Pages 15 - 29)

- System Documentation, Page 16
- Security Plans, Page 20
- Audit Trails, Page 26
- Record Metadata, Page 28



# WHO SHOULD PARTICIPATE?

This *Handbook* encourages collaboration among a variety of subject matter experts to reach the goal of information system trustworthiness. Ideally, workgroups of people with diverse skills and knowledge will work together in this process, including those who have:

- ★ Knowledge of agency business, policies and procedures. This includes directors, administrative services/ administrative managers, assistant attorney generals, and auditors.
- ★ Knowledge regarding information access, retention and data practices. These staff know who can access the information and for what reasons, and how long information must be accessible. This includes agency records officers/custodians, administrative managers and records management.
- ★ Skills in information technology and systems design. These staff can provide advice and propose options on what technologies and methodologies work best to accomplish business needs. This includes Enterprise Technology Services staff, department technologists, and perhaps selected vendors.

The team should first be educated and made aware of the importance of information system trustworthiness and why the evaluation process is necessary. The work group also needs to know the value of documenting its decisions, and staff should be kept apprised of system development progress.

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



# METADATA & DOCUMENTATION

Documentation (Criteria #1) and metadata (Criteria #4) serve as the cornerstone of any trustworthy information system, enabling proper data creation, storage, retrieval, use, modification, retention and destruction.

Metadata is simply data about data. Metadata consists of a structured format and controlled vocabulary that allow for the precise description of record content, context and structure. Metadata includes attributes like file type, file/creator name, date of creation, and use restrictions. Metadata elements describe the object in a standardized way that facilitates information retrieval and administration. Metadata capture, whether automatic or manual, is a process built into the information system.

Documentation has two meanings. Broadly, 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.

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



Would you trust this record keeping system?

# METADATA & DOCUMENTATION

From the initiation of your examination process, irrespective of where in the system development life cycle you begin, you must retain documentation. Documentation procured later in the cycle is fraught with incompleteness and/or errors. Begin by gathering such information including:

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



After you conclude the examination protocol, you will 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 regularly updating your documentation, management can attest to and provide evidence of system trustworthiness in the event of an audit or investigation.



**Red Flag:** Complete documentation of an entire system is a challenging task that may not always be necessary for your particular situation—perhaps only certain functions require this careful attention. The value of your records must be weighed against costs and risks. *How Important is Your Information?* on the following page addresses these considerations.

# HOW IMPORTANT IS YOUR INFORMATION?

Records and data vary in value and the systems that contain your institutional assets and organizational lifeblood require differing levels of security and trustworthiness. To determine the importance of your information you may want to consider the following:

- What state laws and regulations apply to your data?
- What are your agency's accepted standards for system/data security?
- What records retention schedules apply to your information?
- In the event of litigation, what records would lawyers target?
- What information cannot be released to the public?
- What records would Legislative Audit, OMB, or regulators demand?

Certain resources, such as the *Alaska Public Records Act* (AS 40.21), Archives & Records Management regulations (4 AAC 59.005 Electronic Records Retention & Preservation), and your agency's program records retention schedule (*Refer to Bibliography & References, Page 47*) determine the precise importance and security level of your information.

The Public Records laws, however, are written without respect to storage medium or file format and agencies must administer their information assets for the full retention period as stipulated on the *General Administrative Records Retention Schedule* or a program records schedule.



# HOW IMPORTANT IS YOUR INFORMATION?

State agencies should determine the significance of their records, their functional priorities, and the resources available to them in order to make pragmatic decisions about the appropriate practices to apply to its information systems. The *TIS* design criteria set (pages 15 thru 29) will help agencies manage the risks associated with their information systems. While comprehensive in scope, the set does not apply to all systems equally. A system containing purchase orders, for example, will not have as high a legal profile and need for security and trustworthiness as one containing confidential medical records carrying a 20-year retention.

The chief executive officer of each agency may have to prove that her agency has made informed, appropriate choices regarding its records administration and that accountable staff adhere to established policies and procedures during the normal course of routine business. Lawyers, auditors, or other investigators for instance, may examine information systems in exhaustive detail, looking for things like undocumented delays, variance from documented procedures, and security gaps in terms of system and records access. Agencies in these instances, therefore, can attest that its systems have been fully vetted and that management has made comprehensive, documented assessments concerning the administration of its records.

Indeed, building a *Trustworthy Information System* mitigates liability and risk for the agency!



This is not an acceptable record keeping system!

# HOW DO YOU APPLY THE TIS DESIGN CRITERIA?

What are design criteria? Design criteria constitute the explicit goals that a project must achieve in order to be successful. Managers can use these criteria to evaluate the potential for success of an information system project and to determine how well the project fits into the mission of the agency.

The *TIS* design criteria can be used in many ways depending on your agency's particular circumstances. Use of the criteria varies depending upon on a number of agency-specific factors including:

- ▶ Agency information needs, policies and procedures
- ▶ Information system size, type and scope
- ▶ Whether you are phasing criteria into a mature legacy system or are at the initial step of a new system development life cycle
- ▶ Agency size, staff, expertise and resources

When agency information system development teams carefully evaluate the *TIS* design criteria set choices delineated on pages 15 thru 29 questions to ask include:

- ▶ What criteria items are essential to conduct state business and meet information requirements?
- ▶ What are the costs of implementing selected criteria?
- ▶ What governance, risk, and compliance associated costs might be incurred if certain criteria are not completely implemented.?

Agencies have different information needs and operate under different policy mandates and statutes. What's critical to one agency may have little relevance to another.

# HOW DO YOU APPLY THE TIS DESIGN CRITERIA?

When can you apply the design criteria? Obviously, establishing the trustworthiness of an information system is a process most easily undertaken during the analysis/planning phase before the system is rolled out.

The steps, in this instance, are to:

1. Determine the value of your data
2. Weight that value against the time and financial costs of implementing each criteria
3. Implement
4. Document your choices and actions
5. Reassess needs and risks annually

The design criteria set can also be used to examine systems that are already in place—your legacy systems. Examination of this documentation can serve as a check on how well the system meets your various requirements. The steps in this situation are to:

1. Decide upon the value of your data
2. Examine your system vis a vis the criteria and determine which criteria are already addressed
3. Evaluate whether your current system configuration offsets your risks
4. Choose additional criteria for implementation after weighing the costs
5. Implement
6. Document your choices and actions
7. Reassess needs and risks annually

# WHAT ARE THE DESIGN CRITERIA FOR A TIS?

The design criteria are essential for implementing a trustworthy information system. It is important to justify and document decisions to ensure consistent application and provide institutional accountability.

The design criteria are categorized into four main groups:

- #1. System Documentation
- #2. Security Plan
- #3. Audit Trails
- #4. Record Metadata

## **Systems Development Life Cycle Checklist [comment & explain for each]**

- Do laws and/or regulations apply to your system data? Which ones?
- Does the proposed electronic system create data or information that can be identified as a state record under the *State Records Act* (AS 40.21) and in accordance with Archives & Records regulations (4 AAC 59.005, Retention & Preservation of Electronic Records)?
- Does the proposed system provide for appropriate management of records over the full records lifecycle (creation/receipt, maintenance, use, and final disposition) in electronic format?
- Has the agency integrated the management of the electronic records with other records and information technology resources of the department?
- Are there industry standards for your system security?
- Will lawyers target specific areas or types of records?
- Will auditors target specific areas or types of records?
- Is any data of enduring historical value to you or others?

# DESIGN CRITERIA GROUP 1

## SYSTEM ADMINISTRATORS SHOULD MAINTAIN COMPLETE & CURRENT DOCUMENTATION OF THE ENTIRE SYSTEM

- I. System documentation should describe the requirements, capabilities, limitations, design, operation, and maintenance of the system. Includes:
  - A. Hardware, Software, & Communication Networks:  
Procurement, installation, modifications/upgrades and maintenance.
  - B. Interconnected Systems:
    - 1. Types of interconnected systems
    - 2. Names of systems and unique identifiers
    - 3. Owners
    - 4. Names and titles of authorizing personnel
    - 5. Indication of system of record
    - 6. Security protocols and issues

### System Development Life Cycle Checklist [comment & explain for each]

- Does the system possess a unique identifier and/or common name?
- Is a particular agency legally responsible for the system?
- Is a particular agency legally responsible for each application?
- Is the name, job title and contact information of the person(s) responsible for system administration readily available?
- Is the name, job title and contact information of the system security administrator readily available?
- Has a formal risk assessment of the system been completed? When? Performed by whom? Methodology? Findings?
- Is application software properly licensed for all copies in use?

# DESIGN CRITERIA GROUP 1

- Is the Agency records officer [Authority: AS 40.21.060(9) & 4 AAC 59.010] included from the beginning of the system design process?
- Is the Agency records officer included in project status meetings as needed/appropriate?
- Are records identified that support the business process?
- Do current records retention schedules apply to the new system?
- Is a new records schedule required because of a change in records administration?

## Consider:

- System documentation (diagrams, schematics, design reviews, system tests, workflow charts, usage/inventory reports, application software licenses/agreements, security information) are listed on the *General Administrative Records Retention Schedule* along with retention parameters.
- Unique names and identifiers should remain the same over the information system life cycle, as far as is practicable.
- When a system is installed at multiple sites, each site should run a documented, up-to-date version of the authorized configuration.
- Maintain audit trails and documentation of hardware and software changes which identifies individual components of the system at given points in time.
- Ensure that only properly vetted and authorized individuals can make changes to the system.

# DESIGN CRITERIA GROUP 1

## II. Document policies and procedures for:

- A. Programming conventions.
- B. Development and testing activities.
- C. Applications. May include associated methodology regarding data—entering, accessing, modifying, duplicating, and deleting—along with indexing parameters, outputs, and query/report processing.
- D. Identification of when records become official.
- E. Record formats and codes.
- F. System backups. Each appropriately labeled backup should be stored in a secure, offsite location subject to periodic integrity tests.
- G. Quality assurance/control checks and performance/reliability tests of hardware and software on a schedule established through consultation with project team and manufacturers.
- H. Migration of records to new systems and media, as necessary.
- I. Standardized training for all system users.

# DESIGN CRITERIA GROUP 1

## Consider:

- Audit identification devices (security badges/cards, RFID tags) ensure personal verification and system privilege levels.
- Each type of storage medium used should undergo regular statistical sampling following established procedures that outline sampling methods, identify data loss and corresponding causes, and correct identified problems.
- Periodic functional tests should include anomalous as well as routine conditions, and be documented so that any knowledgeable programmer can perform them.
- All executive branch public employees are required to read and sign the *State Policy Regarding Personal Use of State Office Technologies* as a condition of their employment. This policy documents that staff are aware of prohibited uses of office technologies and is located here:  
<http://www.state.ak.us/local/akpages/ADMIN/info/policy/offpol.pdf>

# DESIGN CRITERIA GROUP 2

## SYSTEM ADMINISTRATORS SHOULD DEVELOP A SECURITY PLAN

### I. Establish, document, and implement a security plan

An agency security plan ensures that all information assets—networks, facilities, information systems/groups of information systems—are adequately protected. The preparation of an information system security plan guarantees that required security controls (planned or in situ) are fully documented. The security plan also provides a complete characterization or description of the system [refer also to Criteria 1]. Attachments may include reference to key documents supporting the agency's information security program (e.g., configuration management plan, contingency plan, incident response plan, security awareness and training plan, rules of behavior, risk assessment, security test and evaluation results, system interconnection agreements, security authorizations/accreditations, and plan of action and milestones.) Security plans for information systems currently in operation may require the development of additional security controls to supplement controls already in place or modification of selected controls deemed to be less than effective. Relevant agency security plans and safeguarding procedures at a minimum should include:

#### A. Physical Security

##### 1. Document adequate physical security measures for the protection of physical and logical assets. Issues include:

- a) Access to rooms with terminals, servers, wiring, back-up media
- b) Data interception
- c) Mobile/portable units such as blackberries, laptops, cell phones, other personal digital assistants
- d) Structural integrity of building
- e) Fire safety
- f) Supporting services such as electricity, heat, air conditioning, water, sewage, etc.

# DESIGN CRITERIA GROUP 2

## B. User Authentication, Authorization & Accountability

1. Establish procedures for issuing and revoking accounts. Document user identification, authentication, and access control procedures.
2. Each user's unique identifier and password should be managed within the agency by a system of network and application server directories and directory-enabled applications.
3. Institute password rules. Recommended rules include a minimum of 8 characters (one alpha character, one numeric character, one special character (^ ! @ \$ % ^ & ( ) - \_ = + [ ] ; : ' " , > . > ?), a combination of upper/lower case characters, and expiration dates. Number of log-on attempts should be controlled and system administrators should determine what level and frequency of log-on error constitutes caution and resultant security staff action. Other restrictions on password restrictions may also be implemented.

Poorly chosen passwords include:

- a) Your login ID
- b) Names of co-workers, pets, family, etc.
- c) Phone numbers, license numbers, or birthdays
- d) Simple passwords liked "asdf" (adjacent keys on a keyboard)
- e) Words contained in a dictionary

# DESIGN CRITERIA GROUP 2

## System Development Life Cycle Checklist [comment & explain for each]

- Does a creator, current owner, or system administrator grant access permissions to a record?
- Is there a help desk or specific staff member available to respond to security incidents in a timely manner?
- Is system performance monitoring used to identify the nature and scope of resource shortages that are causing performance problems so that appropriate courses of actions (normally performance tuning and/or the procurement of additional hardware) are taken to resolve the problem?
- Is there a list of all internal and external user groups and the types of data created and/or accessed?
- Have appropriate security classifications/levels been established for all positions?
- Does your agency have security procedures regarding the re-use of excessed storage media so that confidential data is not compromised?

### Consider:

- Refer to NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems, Information Security*; NIST SP 800-65, *Security Considerations in the Information System Development Life Cycle*; NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*; Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems*.

# DESIGN CRITERIA GROUP 2

## C. System Security

System security is a process that demands constant vigilance and failure to properly maintain, configure and update enterprise software can defeat security system capabilities. Develop an information security strategy, as failing to secure government information exposes your agency to numerous risks, including:

- Lost or corrupted information
- Misappropriated and misused data
- System failure, resulting in downtime
- Jeopardizing integrity of information assets
- Theft of electronic personal information, property or assets
- Disruption of enterprise transactions and loss of public confidence
- Violation of privacy (*Article 1, Section 22, Alaska Constitution*)
- Diminished office productivity
- Tarnished reputation due to leak of privileged, confidential or restricted information.

### 1. Internal System Security

- a) Control and monitor access to system documentation.
- b) Control and monitor access to output and storage devices.
- c) Ensure proper data security levels through controls when archiving, purging, copying or moving data from system to system. Employ controls regarding the transportation or mailing of media or printed output. Execute powerful data encryption and program time-outs.
- d) Implement procedures to ensure complete sanitization/wiping and secure disposal of obsolete or superceded hardware, software, and storage media in accordance with ETS directives.
- e) Constantly monitor the system via anomaly detection mechanisms/techniques that flag observed activities that deviate significantly from established normal usage profiles.

# DESIGN CRITERIA GROUP 2

- f) Review security procedures and rules semi-annually to maintain currency.
- g) Train security administration personnel to ensure full understanding of security system operation.

## 2. External System Security

- a) Secure your web site/portal against physical, syntactic (language rules) and semantic (use of incorrect information damaging resource) attacks. The right people should have the right access with minimal loss of flexibility and performance based on user identity, role and the resource or application being accessed.
- b) For records originating outside the system, the system should be capable of verifying their origin and integrity. At a minimum the system should:
  - (1) Verify the identity of the sender or source.
  - (2) Verify the integrity of, or detect errors in, the transmission of information content of the record.
  - (3) Detect changes in the record since the time of its creation or the application of a digital signature.
  - (4) Detect and prevent attacks such as viruses, worms, bots and scanners through the installation and regular updating of computer security and anti-virus/hacker/spyware software placed on all workstations.
- c) Construct firewalls to give users secure online access as well as to separate your agency public Web server from the internal network.

## D. Risk Assessment

- 1. The Department security coordinator, in collaboration with the State security officer, should perform a risk analysis of potential security threats to IT resources annually and provide the results to senior management.

# DESIGN CRITERIA GROUP 2

## E. Disaster, Security Incident Recovery & Continuity of Operations Plans

Disaster, security incident recovery and continuity of operations plans (COOP) should be reviewed annually for currency and tested for efficiency.

1. The agency security coordinator should establish a disaster recovery plan.  
Hazards include:

- a) Fire and/or explosion
- b) Water or flood
- c) Wind or tornado
- d) Lightning
- e) Power outage
- f) Rodents
- g) Insects
- h) Human error
- i) Sabotage, violence and/or terrorism
- j) Acts of God
- k) Other localized acts of nature

2. The agency security coordinator should establish security incident protocols. Hazards include:

- a) Hardware, software, or network failure or malfunction
- b) Human error
- c) Unauthorized access and activity

3. The agency security coordinator should establish a continuity of operations or business resumption plan that includes procedures for various disaster scenarios, both natural and man-made, based upon an initial agency risk assessment.

# DESIGN CRITERIA GROUP 3

## SYSTEM ADMINISTRATORS SHOULD ESTABLISH AUDIT TRAILS THAT ARE MAINTAINED SEPARATELY & INDEPENDENTLY FROM THE OPERATING SYSTEM

- I. Audit trails consist of transaction records in information systems that provide verification of system activity. Without an audit trail, litigators can question the authenticity of a file, which can be used to suggest that it may have been altered to change the data or image. The simplest audit trail is the transaction itself. If a person's salary is increased, the change transaction includes the date, amount of raise, and name of authorizing manager. General characteristics of audit trails include:
- A. Audit trail software and mechanisms subject to strict access controls and protected from unauthorized modification or circumvention.
  - B. Item counts and hash totals verifying that all input has been processed through the system.

### System Development Life Cycle Checklist [comment & explain for each]

- Are certain staff designated to access audit data? Alter? Delete? Add?
- Are certain staff designated to read audit logs? Who?
- Are tools available to output audit information? What are the formats? Who can do this?
- Are there mechanisms available to designate which activities are audited? Who can do this?
- Are audit logs protected? How?

# DESIGN CRITERIA GROUP 3

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

- A. User identifier
- B. Successful/unsuccessful log-ins
- C. Use of password changing procedures
- D. User ID lock-out record
- E. Date
- F. Time
- G. Physical location

III. A system should be in place to log and track users and their online actions. Web server logs and detailed audit trails of portal events might include:

- A. Details of log-in (request date/time, physical location, etc.)
- B. Creation of files/records
- C. Client IP address
- D. Page requested
- E. HTTP code
- F. Bytes served
- G. Accessioned file/record identifiers and accompanying activity (deletion, modification, change of sensitivity/security level)
- H. Accessed device identifiers
- I. Software used
- J. Production of printed output
- K. Output to storage devices

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

- A. Record identifier
- B. User identifier
- C. Date
- D. Time
- E. Usage (e.g., creation, capture, retrieval, modification, deletion)

# DESIGN CRITERIA GROUP 4

## EACH RECORD SHOULD HAVE AN ASSOCIATED SET OF METADATA

### I. What is metadata? [refer also to pp. 9 & 10]

- A. Email header information (possibly hidden)
- B. Proprietary features of word processing (i.e. summary fields)
- C. Embedded and shadow data (fringe data that remains on a track)
- D. Deleted keystrokes
- E. Tracking information
- F. Spreadsheet formulae

### II. Metadata for State electronic records should include, at a minimum:

- A. Custodian of the record
- B. Creation date
- C. Citation to an appropriate records retention schedule stipulating disposition timeframe

### III. Metadata for Alaska electronic records may also include:

- A. Unique identifier
- B. Creation time
- C. Creator's identification/authorization documentation
- D. Modification date/time
- E. Modifier's identification/authorization documentation
- F. Indication of authoritative version
- G. Identification of originating system
- H. Date/Time of receipt from outside system
- I. Addressee
- J. System or mechanism used to capture record from outside system
- K. Protection method
- L. Format
- M. Location of record
- N. Sensitivity classification
- O. Retention period event trigger
- P. Record purge data and disposition

# DESIGN CRITERIA GROUP 4

## System Development Life Cycle Checklist [comment & explain for each]

- Are the components of a complete or final record of a transaction captured?
- If you went to court or had to produce information pursuant to a discovery subpoena or public records request, does the metadata captured protect the State?
- Are there 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?
- Are certain staff designated access to record metadata?  
Can they alter, delete, or add to it?

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Accountability</b>	The quality of being responsible, answerable; the obligation to bear the consequences for failure to perform as expected.
<b>Architecture</b>	An enterprise-wide architecture is a logically consistent set of principles and standards that guide the design and development of an organization's information systems and technology infrastructure.
<b>Archival Value</b>	The ongoing usefulness or significance of records, based on the evidential or informational value that justify their continued preservation.
<b>Archiving</b>	Copying files to long-term storage for backup purposes.
<b>Audit Trail</b>	An electronic means of tracking interactions with records within an electronic system so that any access to the record within the system is documented.
<b>Authenticity</b>	Ensures that a record will be legally admissible and reliable throughout its life cycle.
<b>Authentication</b>	The process of identifying an individual, usually based on a username and password. Authentication ensures that the individual is who he/she claims to be, but says nothing about the access rights of the individual.
<b>Backup/Recovery</b>	Backing up content in various formats and/or locations to ensure business viability in the event of a disaster.
<b>Backward Compatible</b>	Refers to hardware or software that is compatible with previous versions of the product. Also called "downward compatible."

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Biometric-based Device</b>	Authentication techniques that rely on measurable physical characteristics of the user that can be automatically verified. Examples include fingerprint, retina, or face scanners.
<b>Bit</b>	[binary digit].The smallest element of computer storage—a single digit in a binary number, <i>0</i> or <i>1</i> . It is a positive or negative magnetic spot on disk and tape, and charged cells in memory.
<b>Bitmap (BMP Files)</b>	A low quality digital image file format, used most often in word processing applications. BMP format is a binary representation that creates a lossless compression. File extension-- <i>.bmp</i> .
<b>Business Process Analysis (BPA)</b>	Sometimes referred to as Business Analysis, BPA is the performance of a formalized set of tasks, knowledge, and techniques used to identify business needs and to find solutions to business problems. BPA is also an effective tool for identifying and incorporating records management requirements into agency process and systems at the right time because records may be created at any step of the process.
<b>Business Process Management (BPM)</b>	A tool that moves content throughout an identified business process. BPM solutions are used to develop, deploy, monitor, and optimize multiple types of process automation applications, including processes that involve both systems and people.
<b>Byte</b>	Eight binary digits, or cells.
<b>Capture</b>	Scanning, registration, classification, indexing and storage of an item of content in a CMS.
<b>Checksum</b>	A count of the number of bits in a transmission unit that is included with the unit so that the receiver can check to confirm whether the same number of bits arrived. If the counts match, then one can assume that the complete transmission was received.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Compact Disc (CD)</b>	A type of optical disk storage media, cd's come in a variety of formats including CD-ROM (read only); CD-R (write once read only); and CD-RW (re-writable)
<b>Compound Document</b>	A document with multiple elements that may include images, text, animation and hypertext.
<b>Compression</b>	A process, using special software, that reduces the file size of a given electronic file.
<b>Confidentiality [44 USC 3542]</b>	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
<b>Content</b>	Primarily paper documents that have been scanned and indexed. Also includes electronic files stored in a variety of formats and available for retrieval, reuse, and publication.
<b>Content Management System (CMS)</b>	Commercial software that has been adopted and modified to meet an organization's business needs for efficient storage and retrieval of documents and other unstructured data under policy and statutory requirements.
<b>Conversion</b>	Changing a record's file format, often to make the record software-independent and in a standard or open format.
<b>Data</b>	Consists of distinct pieces of information, usually formatted in a special manner--text, numbers, images videos, audio, software, algorithms, equations, animations, models, simulations way. Data assert facts but provide no context for those facts and can be conceptualized as information evidencing any act, transaction, occurrence, event, or other activity.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Data Model</b>	A diagram that shows the various subjects about which information is stored, and the relationships between those subjects.
<b>Data Warehouse</b>	A collection of integrated data designed to support management decision making that presents a coherent picture of business conditions at a single point in time.
<b>Digital</b>	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 Audio Tape (DAT)</b>	A magnetic tape technology used for backing up data. DAT uses 4mm cartridges that conform to the DDS (Digital Data Storage) standard.
<b>Digital Signature</b>	A digital code authenticating an electronic message by uniquely identifying the sender. The purpose of a digital signature is to guarantee that the individual sending the message really is who he/she claims to be.
<b>Digital Versatile Disk (DVD)</b>	An optical disk with more storage capacity than CD-ROM's, also called digital video disks, but do not necessarily include video. Common types of DVD's include: DVD-ROM (read only); DVD-RAM (rewritable); DVD+RW (competitor to DVD-RAM with similar functionality and slightly greater storage capacity).
<b>Disaster</b>	An unexpected occurrence (flood, fire, earthquake, act of terrorism) that inflicts widespread destruction and distress on an agency. Business operations are negatively effected for a long time.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Disaster Recovery Plan</b>	A plan for business continuity in the event of a disaster that destroys part or all of a business's resources, including IT equipment, data, records and the physical space of an organization.
<b>Disposal Date</b>	The date on which the records retention period for a given records series expires and the records may be disposed, either by destruction or transfer to the Alaska State Archives.
<b>Disposition</b>	Either the destruction of a record or the transfer of the record to the Alaska State Archives.
<b>Document</b>	A document conveys information and consists of formatted, identifiable information, comprising a medium and a message, having a beginning and an end. May be represented through alphanumeric text, vector data, a digital map, spreadsheets and databases, moving images or audio data. An electronic document can be conceptualized as the physical embodiment of information or ideas
<b>Documentation</b>	The act or process of substantiation by recording actions and/or decisions. Also, records required to plan, develop, operate, maintain, and use electronic records, including: systems/file specifications, codebooks, file layouts, user guides and output specifications.
<b>Dublin Core Metadata Set</b>	A wide used set of metadata elements easily embedded in a web page.
<b>Dynamic</b>	Refers to actions that take place at the moment they are needed rather than in advance.
<b>Electronic</b>	Technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities. Examples include radios, TVs, instruments, computers and telecommunications.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Electronic Document Management System</b>	A software program and supporting hardware that automate and integrate the records management process.
<b>Electronic Mail</b>	Electronic correspondence created or received on an electronic mail system.
<b>Electronic Record</b>	Under AS 40.21.150(4) information that is recorded in machine readable form. An electronic record is produced or stored by electronic means and accurately reproducible.
<b>Electronic Records Management</b>	The application of records management to physical and electronic records via a computer system or application.
<b>Electronic Signature</b>	Under AS 09.80.190(8) 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.
<b>Enterprise</b>	With respect to Information Technology projects, enterprise refers to the executive branch of state government; i.e. an enterprise system is used by all departments.
<b>Enterprise Technology Services (ETS)</b>	ETS, based in the Department of Administration, is the lead IT technical team for the State of Alaska. ETS provides core IT business systems to all state agencies including network, phone, email, and mainframe services.
<b>File</b>	Physical documents such as paper documents in a manila folder. From an IT perspective—a file is an electronic document of a set of related e-records.
<b>File Name</b>	The name assigned by the user to identify a file.
<b>File Path</b>	The location of the file as it is stored in a series of directories or folders.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>File Transfer Protocol</b>	A communications protocol used to transmit files without loss of data.
<b>Firewall</b>	The primary mechanism to prevent unauthorized computer or internal network access. A firewall allows or blocks traffic into and out of a private network or a user's computer. Firewalls provide users secure access to the Internet as well as to separate a company's public Web server from its internal network.
<b>Format</b>	The structure or layout of a record (n). Record formats consist of the fields, shape, size and style of a record. Report formats are the columns, headers, and footers on a page.
<b>Forward-compatible</b>	The ability of a software program to create files that can be read by more advanced versions of the software.
<b>Free-text Search</b>	A document searching function that searches every word in a document or specified group of documents.
<b>Geographic Information System (GIS)</b>	A GIS consists of hardware and software used for storage, retrieval, mapping, and analysis of geographic data. A GIS can be as complex as entire systems using dedicated databases and workstations connected to a network, or as simple as an off-the-shelf application. A GIS is able to combine and overlay separate layers of geographic data, making it a valuable tool for organizations that need to map and analyze spatial information.
<b>Gigabyte</b>	1,024 megabytes—one billion bytes--of digital data.
<b>Graphics Interchange Format (GIF)</b>	A widely used, propriety digital image file format, GIF supports color and grayscale. Limited to 256 colors, GIF's are more effective for images such as logos and graphics rather than color photos or art. A lossless compression, files in GIF end with a <i>.gif</i> extension.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Hard Copy</b>	Printed output. Contrasts with "soft copy" that exists only electronically.
<b>Hypertext</b>	Hypertext is the foundation of the World Wide Web and enables linkage between related information.
<b>Hypertext Transfer Protocol (HTTP)</b>	A protocol commonly used to access resources on the internet.
<b>Imaging</b>	<i>See scanning.</i>
<b>Information</b>	A type of knowledge that can be exchanged and expressed by data, text, codes, computer programs, software, databases, etc. Information has meaning based upon the context of its creation and use.
<b>Information Life Cycle Management (ILM)</b>	A concept from IT which refers to managing records, documents, information, and data in electronic format. ILM is a comprehensive approach to managing the flow of an information system's data and associated metadata from creation and initial storage to the time when it becomes obsolete and is subsequently deleted. It is a combination of processes, applications, and technologies that work together to direct data and files flowing through the e-environment.
<b>Information Governance</b>	The accountability for the management of an agency's information management assets in order to achieve business purposes and compliance with relevant legislation or regulations.
<b>Information System</b>	A computer business application consisting of the database, application programs, processing systems, and manual/machine procedures. Usually contains electronic records, records on electronic media, input/source documents, output records, along with related documentation and indices.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Information System [44 USC 3502]</b>	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
<b>Input Device</b>	A peripheral device that generates input for the computer such as a keyboard, scanner, mouse, or graphics/digitizing tablet.
<b>Integrity</b>	The property of being complete and unaltered.
<b>Internet</b>	The largest network in the world consisting of more than 350 million computers in more than 100 countries covering commercial, academic, and government endeavors.
<b>Intranet</b>	An in-house Website that serves the employees of the enterprise. Although intranet pages may link to the Internet, an intranet is inaccessible to the general public and is protected by a firewall that blocks unauthorized access.
<b>Joint Photographic Experts Group (JPEG)</b>	A digital image file format, JPEG is a lossy compression technique for color and grayscale images. Depending upon the degree of compression, the loss of detail may be visible to the human eye. Files in JPEG end with a <i>.jpg</i> extension.
<b>Kilobyte</b>	1,024 bytes of digital data.
<b>Legacy System</b>	An older application or computer system often located on a mainframe or minicomputer.
<b>Logon</b>	The process of gaining access, or signing in, to a computer system. If access is restricted, the logon requires users to identify themselves by entering a user name, ID number, and password.
<b>Lossiness</b>	The degree to which data is lost during file compression.
<b>Lossless Compression</b>	A data compression technique in which no data is lost.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Lossy Compression</b>	A data compression technique in which some amount of data is lost. Lossy methods provide high degrees of compression and eliminate redundant and unnecessary information.
<b>Magnetic Disk</b>	The primary digital storage media. These random access, rotating platters are magnetically recorded via a mechanical arm with a read/write head and can be re-recorded multiple times. Types include hard/floppy disks and removable cartridges.
<b>Magnetic Tape</b>	A sequential digital storage media, magnetic tapes come in reel-to-reel as well as cartridge format. Tape has been more economical than disks for archival data, but that is changing as disk capacities have increased enormously. If tapes are stored long-term, they must be periodically recopied or the tightly coiled magnetic surfaces may contaminate each other.
<b>Megabyte</b>	1,024 kilobytes—one million bytes--of digital data.
<b>Metadata</b>	Data that describes the content, context, and structure of records and their management thru time. Metadata associated with email may include headers, attachments, date/time, domain names, and recipient lists. Metadata in file systems can provide information about revision lists, retention policies, database field data, modification dates, files sizes and authors; and, documents created by popular office programs such as Microsoft Word and Excel can include embedded document information such as changes made, deletions and reviewer names.
<b>Metadata Model</b>	A general framework for organizing the presentation and entry of metadata.
<b>Microform</b>	In micrographics, a medium that contains microminiaturized images such as microfiche and microfilm.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Migration</b>	Moving data, applications and files to another storage system or computer platform while maintaining the records' authenticity, integrity, reliability, and usability. File format changes may be required.
<b>Moore's Law</b>	The number of transistors per square inch on integrated circuits doubles about every 18 months. Data densities (memory capacities) and processing power (speed) is linked to this law. Holds true for another two decades.
<b>Nearline Storage</b>	Available within a short amount of time, but not instantly. Storage in a system that is not a direct part of the network in daily use, but that can be accessed through the network.
<b>Offline Storage</b>	The storage of digital data (tape and disk) in a data library. Offline data cannot be accessed from a computer or terminal until it is mounted in the drive.
<b>Online Storage</b>	The storage of digital data as fully accessible information on the network.
<b>Optical Character Recognition (OCR)</b>	The machine recognition of printed characters. This involves analysis of the scanned-in image, and then translation of the character image into character codes, such as ASCII. OCR creates text-searchable files for digital collections and can be utilized to process checks and credit cards, and sort mail.
<b>Petabyte</b>	One quadrillion bytes of data—one trillion kilobytes.
<b>Pixel</b>	The smallest addressable unit on a display screen or raster-based graphics file. Derived from <i>picture element</i> .
<b>Pixel Bit-Depth</b>	Defines the number of shades that can be represented by the amount of information saved for each pixel. These can range from 1 bit/pixel for binary (fax type) images to 24 bits/pixel or greater for high quality color images.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Portable Document Format (PDF)</b>	The de facto standard for document publishing developed by Adobe, commonly used to capture, distribute, and store electronic documents. Preserves the fonts, images, and graphics of the original digital files. Files in PDF often end with a <i>.pdf</i> extension and may be viewed across multiple platforms.
<b>Public-Key Encryption</b>	A cryptographic system that uses two keys -- a <i>public key</i> known to everyone and a <i>private</i> or <i>secret key</i> known only to the recipient of the message.
<b>Public Record</b> under AS 40.25.220(3)	Books, papers, files, accounts, writings, including drafts and memorializations of conversations, and other items, regardless of format or physical characteristics, that are developed or received by a public agency, or by a private contractor for a public agency, and that are preserved for their informational value or as evidence of the organization or operation of the public agency.
<b>Raster Graphics</b>	The representation of a digital image as a matrix of pixels. Also called bitmapped images. Formats include JPEG, GIF, BMP, and TIFF.
<b>Record</b> under AS 40.21.150(6)	Any document, map, plat, photo, microfilm, magnetic tape, electronic record... regardless of physical form or characteristic, developed or received under law or in connection with the transaction of official business preserved as evidence of the organization, function, policies, decisions, procedures, operations, or other activities of the state. [see also "public record"]
<b>Recordkeeping</b>	The act or process of creating, maintaining, and disposing of records. Refer also to <i>Records Management</i> .

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Records Management</b>	The planning, controlling, directing, organizing, training, promoting, and other managerial activities related to the creation, maintenance, use, and disposition of records. Refer also to <i>Recordkeeping</i> .
<b>Records Retention Period</b>	The length of time a given records series must be kept, expressed as either a time period (e.g. 4 years); a cut-off event (e.g. file closure) or action (e.g. audit); or, a combination (e.g. 6 months after audit concluded).
<b>Records Retention Schedule</b>	A concise, official guide providing mandatory instructions for the management of an Agency's records including: records series description; length of time in office; length of time, if any, in offsite storage; and, disposition instructions. Retention schedules are fully authorized by the Agency Head (operational purposes), Attorney General (legal purposes), Commissioner of Administration (financial purposes) and the state archivist (historical purposes).
<b>Records Series</b>	A group of records related by their function, activity, or subject and arranged together because the same forms are used, the physical media is similarly (maps, blueprints, cd's), or the disposition authority is similar.
<b>Redaction</b>	Process of hiding sensitive/confidential information in a record.
<b>Reliability</b>	Reliability refers to a record's authority and is established at record creation. It means that the record is able to stand for the fact it is about.
<b>Removable Media</b>	Media including tapes, disks, drives, flash memory devices, and other portable devices.
<b>Retention Period</b>	Time frame that records must be retained before their final disposition, taking into consideration all legal, operational, and financial values.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Risk</b> [NIST SP 800-30]	The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.
<b>Risk Analysis</b>	The process of defining and analyzing the dangers to individuals, businesses, and government agencies posed by potential natural and human-caused adverse events.
<b>Security</b>	Restricts access to content, both during its creation and management as well as when delivered.
<b>Scanning</b>	The process of producing a digital image from a paper document or record. Increasingly, electronic document images have the same legal status as a paper document.
<b>Spoliation</b>	Destruction of evidence relevant to a legal proceeding.
<b>Spyware</b>	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge.
<b>Storage Device</b>	A peripheral unit or device that holds data such as disk, tape or flash memory card.
<b>Structured Information</b>	Information that has a defined structure and is intended to be processed by a computer. For example, most information held in relational databases and processed by computer programs is considered structured.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Subsystem</b>	A major subdivision or component of an information system consisting of information, information technology, and personnel that perform one of more specific functions.
<b>System Development Life Cycle (SDLC)</b>	A structured and organized process for all phases of information system development that ensures all functional/user requirements and agency strategic goals/objectives are met. Typical phases of the SDLC include: feasibility analysis, system planning, design, development, integration and testing, deployment, production, and retirement.
<b>Tagged Image File Format (TIFF)</b>	A bitmapped graphics file format for storing images. TIFF supports monochrome, gray-scale, and color. TIFF is non-proprietary, offers the option of lossless compression, and allows for OCR analysis. TIFF files usually carry a <i>.tif</i> extension.
<b>Taxonomy</b>	A records taxonomy is a corporate-wide schema for the identification, retrieval, and disposition of all business records.
<b>Terabyte</b>	1,024 gigabytes of digital data—one trillion bytes.
<b>Threat [CNSS Inst. 4009]</b>	Any circumstance or event with the potential to adversely impact agency operations (including mission, function, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
<b>Transaction</b>	An action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.
<b>File Transfer Protocol</b>	A communications protocol used to transmit ASCII text, binary, and other files without data loss.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Trustworthy Information System</b>	An information system that produces reliable and authentic records. Trustworthy denotes faith, ability, integrity, and confidence.
<b>Uniform Resource Identifier (URI)</b>	A short text string that describes an item on the Internet. Also known as the resource's address. The terms URI and URL are used synonymously, but URL is more widely used in everyday conversation
<b>Uniform Resource Locator (URL)</b>	The address that defines the route to a file on an Internet server (Web server, FTP server, mail server, etc.).
<b>Uniform Resource Name (URN)</b>	A type of URI scheme designed to serve as a persistent, location-independent resource identifier.
<b>User [CNSS Inst. 4009]</b>	Individual or system process authorized to access an information system.
<b>Unstructured Information</b>	Information without a fully defined structure, intended to be read and used by humans. For example, most information produced by common office applications such as Microsoft Word is considered unstructured.
<b>Vector Graphics</b>	A representation of a digital image as points, lines, and other geometric shapes.
<b>Version Control</b>	A document management feature that allows users to develop and manage successive drafts of their work in a controlled manner.

# GLOSSARY

<u>Term</u>	<u>Definition</u>
<b>Virus</b>	Software used to infect a computer. After the virus code is written, it is buried within an existing program. Once that program is executed, the virus code is activated and attaches copies of itself to other programs in the system. Infected programs copy the virus to other programs.
<b>Vital Record</b>	A record that is essential to the organization's operation or to the reestablishment of the organization after a disaster.
<b>Web Site</b>	An organization's presence or individual's presence on the World Wide Web. A web site is a collection of web pages, which are documents coded in HTML that are linked to each other and very often to pages on other Web sites. A Web site is hosted on a server by its owner or at an ISP.
<b>Web Site Snapshot</b>	The capture of a complete web site as a backup copy using special software.
<b>World Wide Web (WWW)</b>	A system of Internet "Web servers" that store and disseminate "Web pages," which are "rich" documents that contain text, graphics, animations and videos. The documents are formatted in HTML—HyperText Markup Language—that support links to other documents.
<b>Workflow</b>	A tool in content management software that moves content throughout an identified business process. Workflow handles approvals, and prioritizes the order in which documents are presented for approval based on pre-defined business rules.
<b>Worm</b>	A destructive program that replicates itself throughout a single computer or across a network. It can do damage by sheer reproduction, consuming internal disk and memory resources within a single computer or by exhausting network bandwidth. It can also deposit a <i>Trojan</i> for malicious purposes. Often, the terms <i>worm/virus</i> are used synonymously; however, worm implies an automatic method for reproducing itself in other computers.

# BIBLIOGRAPHY & REFERENCES

## Alaska Laws & Regulations

### Alaska Statutes

AS 09.80 (Uniform Electronic Transactions Act)  
AS 11.56.815 - 820 (Tampering with Public Records)  
AS 18.15.365 (Health Information Security Safeguards)  
AS 39.52 (Alaska Executive Branch Ethics Act)  
AS 40.17 (Recording of Documents)  
AS 40.21 (Management & Preservation of Public Records)  
AS 40.25 (Public Record Disclosures)

### Alaska Administrative Code

2 AAC 05.200 - 290 (Verification of Electronic Signatures)  
2 AAC 96.300 - 360 (Requests for Public Records)  
2 AAC 96.400 - 460 (Requests for Electronic Services & Products)  
4 AAC 59 (Archives & Records Management Services)  
11 AAC 53 (Records, Surveys & Platting)

## Alaska Policies, Procedures, Rules, Guidelines & Other Directives

Department of Administration. Enterprise Technology Services. Statewide IT Policies.

- Basic Office Software Minimum Standard Policy
- Disposal of Electronic Media
- Domain Name Request Policy
- Geographic Information Systems Policy
- Computer Network Security Policy
- Statewide Network Policy
- State of Alaska Metadirectory and MIIS Policy
- State of Alaska's Privacy Policy
- Wireless Points of Access

Personal Use of Office Technologies Policy (SP-017). October 1, 2005  
<https://intranet.state.ak.us/admin/sp017.pdf>

# BIBLIOGRAPHY & REFERENCES

Department of Education & Early Development. Division of Libraries, Archives & Museums. Records Management Program.

[http://www.archives.state.ak.us/records\\_management/records\\_management.html](http://www.archives.state.ak.us/records_management/records_management.html)

- General Administrative Records Retention Schedules
- Program Records Retention Schedules
- Records Management Manual
- Email: FAQ & Rules
- Disaster Preparedness & Response Manual

## **Federal Government Laws, Guidelines, Reports & Websites**

US Federal Government. Homeland Security Presidential Directive #12 (Electronic Identification)

<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>

US Federal Government. The National Archives. Records Management Resources.

<http://www.archives.gov/records-mgmt/index.html>

US Federal Government. The National Archives. Toolkit for Managing Electronic Records,

<http://toolkit.archives.gov/pls/htmldb/f?p=102:1:16071237143323062133>

US Federal Government. Department of Commerce. National Institute of Standards & Technology, Technology Administration. Special publications related to computer security, information security testing, virtual private networks, securing external devices for telework, storage encryption technologies, using approved hash algorithms, random hashing digital signatures, etc.

<http://csrc.nist.gov/publications/PubsSPs.html>

US Federal Government. Department of Defense. Records Management Software Applications Design Criteria Standard 5015.2.

<http://jitc.fhu.disa.mil/recmgt/index.html>

US Federal Government. Department of Justice. FBI Electronic Records Certification Manual, 2004.

<http://www.archives.gov/records-mgmt/toolkit/pdf/erkc-manual.pdf>

# BIBLIOGRAPHY & REFERENCES

United States Code. Electronic Signatures in Global & National Commerce Act, 2000. 15USC96.

<http://frwebgate6.access.gpo.gov/cgi-bin/waisgate.cgi?WAIIdocID=09242390979+6+0+0&WAIAction=retrieve>

## Other State Publications & Websites

Arizona. Arizona State Library, Archives & Public Records. Records Management Division. Electronic Record Keeping System Guidelines, 2003

[http://www.lib.az.us/records/GuidanceAndRelatedResources.cfm?GuidanceAndRelatedResources/ers\\_guide.cfm](http://www.lib.az.us/records/GuidanceAndRelatedResources.cfm?GuidanceAndRelatedResources/ers_guide.cfm)

California. Department of General Services. California Records & Information Management (CalRIM) February 2002.

<http://www.osp.dgs.ca.gov/recs/erm.htm>

Delaware. Model Guidelines for Electronic Records, revised December 1, 2003.

[http://archives.delaware.gov/govsvcs/records\\_policies/model%20guidelines.shtml](http://archives.delaware.gov/govsvcs/records_policies/model%20guidelines.shtml)

Kansas Historical Society. Kansas Electronic Records Management Guidelines.

<http://www.kshs.org/government/records/electronic/electronicrecordsguidelines.htm>

Minnesota Historical Society. Minnesota State Archives. Electronic Records Management Resources.

<http://www.mnhs.org/preserve/records/electronicrecords.htm>

Oregon. IT Investment & Planning. Electronic Records Management Systems.

[http://www.das.state.or.us/DAS/EISPD/ITIP/Comm\\_of\\_Practice\\_ERM.shtml](http://www.das.state.or.us/DAS/EISPD/ITIP/Comm_of_Practice_ERM.shtml)

South Carolina Archives & Records Management. Electronic Records Program.

<http://www.state.sc.us/scdah/armer.htm>

Utah. Administrative Services Department, State Archives. Electronic Records.

<http://www.archives.state.ut.us/main/index.php?module=Pagesetter&func=viewpub&tid=1&pid=201>

Washington Secretary of State. Washington State Digital Archives.

<http://www.digitalarchives.wa.gov/default.aspx>

# BIBLIOGRAPHY & REFERENCES

## Other Organizations' Guidelines & Reports

American Bar Association. ABA Legal Technology Resource Center.  
<http://www.abanet.org/tech/ltrc/fyidocs/rm.html>

Association for Information & Image Management. <http://www.aiim.org/>

Association of Records Managers and Administrators, Int'l (ARMA).  
<http://arma.org/>

Australia. National Archives of Australia. Designing & Implementing Record Keeping Systems (DIRKS) Manual, Version 2, 2007.  
<http://www.naa.gov.au/records-management/systems/DIRKS/index.aspx>

Australia. Victorian Electronic Records Strategy (VERS) 2007.  
<http://www.prov.vic.gov.au/vers/standard/version2.htm>

Center for Technology in Government. State University of New York. University at Albany. <http://www.ctg.albany.edu/>

Cohasset Associates, Inc. 3806 Lake Point Tower, 505 North Lake Shore Drive, Chicago IL, 60611. <http://www.cohasset.com/index.html>

Enterprise Content Management Association  
<http://www.aiim.org/standards.asp?ID=28639>

The ePolicy Institute.  
<http://www.epolicyinstitute.com/>

Information Requirements Clearinghouse. Greenwood Village, CO 80111  
<http://irch.com/>

Information Systems Audit & Control Association & Foundation.  
<http://www.isaca.org/>

The Sedona Conference. The Sedona Guidelines: Best Practice Guidelines & Commentary for Managing Information and Records in the Electronic Age, 2004.  
<http://www.thesedonaconference.org/content/miscFiles/RetGuide200409.pdf>

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/AIIM Standards, Technical Reports, & Guidelines

ANSI/AIIM MS52-1991. *Recommended Practice for the Requirements & Characteristics of Original Documents Intended for Optical Scanning.*

ANSI/AIIM MS53-1993. *Recommended Practice: File Format for Storage & Exchange of Image; Bi-Level Image File Format.*

ANSI/AIIM MS54-1993(R1999). *Graphic Symbols for Controls on Document Imaging Equipment.*

ANSI/AIIM MS55-1994. *Identification & Indexing of Page Components (Zones) for Automated Processing in an Electronic Image Management (EIM) Environment.*

ANSI/AIIM MS58-1996. *Standard Recommended Practice for Implementation of Small Computer Systems Interface (SCSI-2), (X3, 131-1994) for Scanners.*

ANSI/AIIM MS59-1996. *Media Error Monitoring & Reporting Techniques for Verification of Stored Data on Optical Digital Data Disks.*

ANSI/AIIM MS60-1996. *Electronic Folder Interchange Datastream.*

ANSI/AIIM MS61-1996. *Application Programming Interface (API) for Scanners in Document Imaging Systems.*

ANSI/AIIM MS66-1999. *Metadata for Interchange of Files on Sequential Storage Media Between File Storage Management Systems (FSMSs).*

ANSI/AIIM TR01-1988 (A1992) *Guidelines for Metrics.*

ANSI/AIIM TR02-1998. *Glossary of Document Technologies.*

ANSI/AIIM TR15-1997. *Planning Considerations, Addressing Preparation of Documents for Image Capture.*

ANSI/AIIM TR17-1989 (A1992). *Facsimile & Its Role in Electronic Imaging.*

ANSI/AIIM TR19-1993. *Electronic Imaging Output Displays.*

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/AIIM Standards, Technical Reports, & Guidelines, continued

ANSI/AIIM TR21-1991. *Recommendations for the Identifying Information to be Placed on Write-Once-Read-Many (WORM) and Rewritable Optical Disk (OD) Cartridge Label(S) and Optical Disk Cartridge Packaging (Shipping Containers).*

ANSI/AIIM TR25-1995. *The Use of Optical Disks for Public Records.*

ANSI/AIIM TR26-1993. *Resolution As It Relates to Photographic & Electronic Imaging.*

ANSI/AIIM TR27-1996. *Electronic Imaging Request for Proposal (RFP) Guidelines.*

ANSI/AIIM TR28-1991. *The Expungement of Information Recorded on Optical Write-Once-Read-Many (WORM) Systems.*

ANSI/AIIM TR29-1993. *Electronic Imaging Output Printers.*

ANSI/AIIM TR31-2004. *Performance Guidelines for Admissibility of Records Produced by Information Technology Systems as Evidence - Part I: Performance Guidelines; Part 2: Acceptance by Government Agencies; Part 3: Implementation.*

ANSI/AIIM TR31/4-1994 (R1999). *Performance Guidelines for Admissibility of Records Produced by Information Technology Systems As Evidence - Part IV: Model Act & Rule.*

ANSI/AIIM TR32-1994. *Paper Forms Design Optimization for Electronic Image Management (EIM).*

ANSI/AIIM TR33-1998. *Selecting an Appropriate Image Compression Method to Match User Requirements.*

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/AIIM Standards, Technical Reports, & Guidelines, continued

ANSI/AIIM TR34-1996. *Sampling Procedures for Inspection by Attributes of Images in Electronic Image Management (EIM) & Micrographics Systems.*

ANSI/AIIM TR35-1995. *Human & Organizational Issues for Successful EIM System Implementation*

ANSI/AIIM TR38-1996. *Identification of Test Images for Document Imaging Applications.*

ANSI/AIIM TR39-1996. *Guidelines for the Use of Media Error Monitoring & Reporting Techniques for the Verification of Information Stored on Optical Digital Data Disks.*

ANSI/AIIM TR40-1995. *Suggested Index Fields for Documents in Electronic Image (EIM) Environments.*

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/ISO/ARMA

ISO 15489-1:2007. *Records Management, Information & Documentation, Part 1: General.*

ISO 15489-2-2002. *Records Management: Part 2: Guidelines & Responsibilities.*

ANSI/ARMA 8-2005. *Retention Management for Records & Information.*

ANSI/ARMA 5-2003. *Vital Records: Identifying, Managing, & Recovering Business-critical Records.*

ISO 10089-1991. *130 mm Rewritable Optical Disk Cartridge for Information Interchange.*

ISO 10090-1991. *90 mm Optical Disk Cartridges, Rewritable & Read Only, for Data Interchange.*

ISO 10149-1995. *Data Interchange on Read-only 120 mm Optical Data Disks.*

ISO 10922-2000. *Information on Optical Disk Cartridges, (ODC) Shipping Packages, & ODC Labels.*

ISO 11560-1992. *Magneto-optical Recorded WORM.*

ANSI X3.213-1994. *86 mm Rewritable Optical Disk Cartridge Using the Discrete Block Format (DBF) Method.*

ISO/IEC 10090-1992. *90 mm Optical Disk Cartridges, Rewritable & Read Only, for Data Interchange.*

ISO/IEC 9171-1;2-1990. *130 mm Optical Disk Cartridge, Write Once, for Information Interchange - Part 1: Unrecorded Optical Disk Cartridge; Part 2: Recording Format.*

ISO/IEC 10089-1991. *130 mm Rewritable Optical Disk Cartridge for Information Interchange.*

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/ISO/ARMA, continued

ISO/IEC 11560-1992. *Information Interchange on 130 mm Optical Disk Cartridges Using the Magneto-optical Effect, for Write Once, Read Multiple Functionality.*

ANSI X3B11/91-120. *WORM Application Using Magneto-optical Media.*

ISO/IEC DIS 13481-1993. *Data Interchange on 130 mm Optical Disk Cartridges - Capacity: 1 Gigabyte per Cartridge.*

ANSI/INCITS 211-1992 (R1997). *130 mm Write-Once Optical Disk Cartridge Using Continuous Servo RLL 2.7 Encoding & LDC.*

ANSI/INCITS 212-1992 (R1997). *130 mm Rewritable Optical Disk Cartridge for Information Interchange.*

ANSI/INCITS 214-1992 (R1997). *130 mm Optical Disk Cartridge Using Sampled Servo & 4/15 Modulation.*

ANSI/INCITS 220-1992 (R1997). *130 mm Optical Disk Cartridges of the Write-Once, Read Multiple (WORM) Type, Using the Magnetic-Optic Effect.*

ANSI/INCITS 191-1991 (R1997). *Recorded Optical Media Unit for Digital Information Interchange - 130 mm Write-Once Sampled Servo RZ Selectable Pitch Optical Disk.*

ISO/IEC 13403: 1995. *Information Interchange on 300 mm Optical Disk Cartridges of the Write Once, Read Multiple (WORM) Type Using the CCS Method.*

ISO/IEC 10885: 1993. *356 mm Optical Disk Cartridge for Information Interchange - Write Once.*

ANSI/INCITS 200-1992 (R1997). *356 MM Optical Disk Cartridge - Write Once, Parts 1 & 2.*

ANSI/INCITS 191-1991 (R1997). *Recorded Optical Media Unit for Digital Information Interchange - 130 mm Write-Once Sampled Servo RZ Selectable Pitch Optical Disk.*

# BIBLIOGRAPHY & REFERENCES

## Media Standards—ANSI/ISO/ARMA, continued

ANSI/INCITS 211-1992 (R1997). *130 mm Write-Once Optical Disk Cartridge Using Continuous Servo RLL 2.7 Encoding & LDC.*

ANSI/INCITS 202-1992 (R1997). *130 mm Rewritable Optical Disk Cartridge for Information.*

ANSI/INCITS 213-1994. *86 mm Disk, 90 mm case, Rewritable Optical Disk Cartridge Using Discrete Block Format (DBF).*

ANSI/INCITS 214-1992 (R1997) *130 mm Optical Disk Cartridge Using Sampled Servo & 4/15 Modulation.*

ISO/IEC 9171-1;2:1990. *130 mm Optical Disk Cartridge, Write Once, for Information Interchange - Part 1: Unrecorded Optical Disk Cartridge; Part 2: Recording Format.*

ISO/TR 12037:1998. *Electronic Imaging -- Recommendations for the Expungement of Information Recorded on Write-once Optical Media.*

ISO/IEC 13346:1999. *Volume & File Structure of Write-once & Rewritable Media Using Non-sequential Recording for Information Interchange.*