

Ohio Trustworthy Information Systems Handbook: Section 9

What are the criteria for a trustworthy information system?

QUESTIONS TO ASK

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

What are your industry's standards for system security?

What are your industry's standards for data security?
What areas/records might lawyers target?

What areas/records might auditors target?

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

Introduction

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 Ohio 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](#)

Ohio Trustworthy Information Systems Handbook: Section 9

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 agency is responsible for the information/data?

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

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

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

Did You Know:

DAS Policy No.: ITP A.26 Effective Date July 1, 2001 Each state agency/organization will develop a Software Copyright Compliance Plan or submit other such procedures accompanied by a certification of the Director of a State Agency that necessary and reasonable controls are in place to assure compliance with applicable manufacturers' license agreements.

DAS Directive No.: 01-25 Effective Date December 27, 1999 "Internet, electronic mail and online services use and abuse" 5. State employees shall not use the Internet, electronic mail and online services to provide access to confidential information. State employees shall not use these services to provide access to public information without following the existing rules and procedures of the custodial agency for dissemination.

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:

Rule 123:3-1-01 of the Administrative Code "Use of

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?

Electronic Signatures and Records" (H) Required Polices. State agencies must establish documented polices and procedures that provide reasonable assurances of authenticity of signatures, the nonrepudiation of the records by the signatories and the integrity of the signed records. This includes but is not limited to polices and procedures on access, control, monitoring, maintenance and any other actions necessary for physical, network and computer security.

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.

Complete audit trails of hardware and software changes should be maintained. This documentation should be extensive enough to identify the individual components of the system at any given point in time.

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 backups being appropriately labeled, stored in a secure, off-line, off-site location, and subjected to periodic integrity tests
7. routine performance of quality assurance and control checks, as well as performance and reliability testing of hardware and software on a schedule established through consultation with the manufacturers

Consider This:

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

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, i.e., every field or informational element of a record, should be migrated to the new system as a single unit.
9. standard training for all users and personnel with access to equipment

Did You Know:

*Ohio Revised Code § 1306.23 Exemptions to disclosure of records
Records that would disclose or may lead to the disclosure of records or information that would jeopardize the state's continued use or security of any computer or telecommunications devices or services associated with electronic signatures, electronic records, or electronic transactions are not public records for purposes of section 149.43 of the Revised Code.*

DAS Policy No.: ITP-E.030 Effective Date May 1, 1999 Electronic records should be created and maintained in reliable and secure systems. Agencies should identify systems that create and maintain records. The development, modification, operation, and use of these systems should be documented and measures should be taken to ensure reliability and security of records over time.

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.

Ohio Trustworthy Information Systems Handbook: Section 9

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?

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:

Ohio Revised Code § 1306.08 When electronic record or signature is attributable to person; effect. (A) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature is attributable.

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:

Ohio Revised Code § 2913.04 Unauthorized use of property; computer or telecommunication property. (B) No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, telecommunications device, telecommunications service, or information service or other person authorized to give consent by the owner.

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.

How is information purged from the system?

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

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.

Did You Know:

Ohio Revised Code § 2913.49 Taking the identity of another. No person shall obtain, possess, or use any personal identifying information of any living or dead individual with the intent to fraudulently obtain credit, property, or services or avoid the payment of a debt or any other legal obligation.

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.

Did You Know:

Ohio Revised Code § 2913.42 Tampering with records. (A) No person, knowing the person has no privilege to do so, and with purpose to defraud or knowing that the person is facilitating a fraud, shall do any of the following: (1) Falsify, destroy, remove, conceal, alter, deface, or mutilate any writing, computer software, data, or record;

6. Access to private keys for digital signatures should be limited to authorized individuals.
7. Lists of all current and past authorized users along with their privileges and responsibilities should be maintained. The current list should be reviewed on a regular schedule to ensure the timely removal of authorizations for former employees, and the adjustment of clearances for workers with new job duties.

Did You Know:

DAS Directive No.: 01-25 Effective Date July 1, 2001 "Internet, electronic mail and online services use and abuse" 6. State employees shall not use an Internet, electronic mail or online service account or signature line other than their own.

8. In order to avoid any real or perceived conflict of interest, one should avoid situations in which the individual responsible for the security of a system also has a strong personal interest in the records held within the system.

2B. Internal System Security

1. Access to system documentation should be controlled and monitored.

Did You Know:

Ohio Revised Code § 1306.23 Exemptions to disclosure of records. "Records that would disclose or may lead to the disclosure of records or information that would jeopardize the state's continued use or security of any computer or telecommunications devices or services associated with electronic signatures, electronic records, or electronic transactions are not public records for purposes of section 149.43 of the Revised Code."

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.

C. 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.

Did You Know:

Ohio Revised Code § 2909.04 Disrupting public services. (A) No person, purposely by any means or knowingly by damaging or

tampering with any property, shall do any of the following: (1) Interrupt or impair television, radio, telephone, telegraph, or other mass communications service; police, fire, or other public service communications; radar, loran, radio, or other electronic aids to air or marine navigation or communications; or amateur or citizens band radio communications being used for public service or emergency communications;

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:

Ohio Revised Code § 2913.04 Unauthorized use of property; computer or telecommunication property. (B) No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, telecommunications device, telecommunications service, or information service or other person authorized to give consent by the owner.

DAS Policy No.: ITP E.8 Effective Date January 1, 1996 2. Vandalism and Related Crimes. An employee does not have to actually remove property to violate a provision of the Ohio Criminal Code. The Vandalism statute, R.C. 2909.05 (B) (2). Provides that: "no person shall knowingly cause serious physical harm to property that is owned, leased, or controlled by a governmental entity." This includes "the intentional introduction of a 'worm' or 'virus' into a publicly owned computer network."

Criteria Group 3

Ohio Trustworthy Information Systems Handbook: Section 9

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.

Did You Know:

Ohio Revised Code § 2913.04 Unauthorized use of property; computer or telecommunication property. (B) No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any computer, computer system, computer network, telecommunications device, telecommunications service, or information service without the consent of, or beyond the scope of the express or implied consent of, the owner of the computer, computer system, computer network, telecommunications device, telecommunications service, or information service or other person authorized to give consent by the owner.

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

Did You Know:

Ohio Revised Code § 1306.11 Requirement that record be retained; checks. (A) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record if both of the following are satisfied: (1) The electronic record accurately and completely reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise. (2) The electronic record remains accessible for later reference. (F) A record retained as an electronic record in accordance with division (A) of this section satisfies a law requiring a person to retain a record for evidentiary, audit, or similar purposes, unless a law enacted after the effective date of this section specifically prohibits the use of an electronic record for the specified purpose.

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

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)

Did You Know:

Ohio Revised Code § 1306.20 State agency provisions. (E)(1) To the extent a state agency retains an electronic record, the state agency may retain a record in a format that is different from the format in which the record was originally created, used, sent, or received only if it can be demonstrated that the alternative format used accurately and completely reflects the record as it was originally created, used, sent, or received. (2) If a state agency in retaining any set of electronic records pursuant to division (E)(1) of this section alters the format of the records, the state agency shall create a certificate of authenticity for each set of records that is

altered. (3) The department of administrative services, in consultation with the state archivist, shall adopt rules in accordance with section 111.15 of the Revised Code that establish the methods for creating certificates of authenticity pursuant to division (E)(2) of this section.

[Criteria Group 4](#)

[Go to Table of Contents](#)

Ohio Trustworthy Information Systems Handbook: Section 9

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.

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

Did You Know:

DAS Policy No.: ITP E.7 Effective Date July 1, 1994 All state executive branch agencies are expected to have a business resumption plan on file at their agency by July 1, 1995. The plan shall be tested and updated at least annually to assure its validity.

2. 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. Federal Emergency Management Agency (FEMA), emergency response and recovery guidelines available at: [http://www.fema.gov/r-n-r/ers_wl.htm#]
3. See also Federal Information Processing Standards Pub. 87 "Guidelines for ADP Contingency Planning"

Ohio Trustworthy Information Systems Handbook: Section 9

Criteria Group 5:

Each record 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

5A. The metadata for each record may include:

1. unique identifier

Consider This:

One method of identification is to have the system automatically assign unique consecutive numbers with time-date stamps to the individual units of storage media as they are written to for the first time, thus prohibiting the addition of false units or the removal of legitimate ones from the storage series.

Many systems assign new identifiers to modified records.

2. date of creation
3. time of creation
4. creator's ID and agency / organization
5. documentation of creator's authorization
6. date of modification
7. time of modification
8. modifier's ID and agency / organization
9. documentation of modifier's authorization
10. indication of authoritative version
11. identification of originating system
12. date of receipt from outside system
13. time of receipt from outside system
14. addressee

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?

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?

15. system or mechanism used to capture record from outside system
16. protection method
17. media type
18. format
19. location of record
20. sensitivity classification
21. retention period event
22. retention period
23. disposition action

Did You Know:

DAS Policy No.: ITP E.30 Effective Date May 1, 1999 Electronic records should be created and maintained in reliable and secure systems. Agencies should identify systems that create and maintain records. The development, modification, operation, and use of these systems should be documented and measures should be taken to ensure reliability and security of records over time.

Ohio Revised Code § 1306.21 Rules for state agency use. (A) With regard to state agency use of electronic records or electronic signatures, the department of administrative services, in consultation with the state archivist, shall adopt rules in accordance with section 111.15 of the Revised Code setting forth all of the following: (1) The minimum requirements for the method of creation, maintenance, and security of electronic records and electronic signatures;

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.

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?

[Glossary](#)

[Go to Table of Contents](#)