OhioDAS

State of Ohio Administrative Policy

Electronic Records

No:
Information Technology
IT-07

Effective:
October 13, 2016

Issued By:

Robert Blair, Director

1.0 Purpose

The purpose of this electronic ***records*** policy is to (a) establish uniform electronic records guidelines for all state agencies; and (b) support the creation and maintenance of electronic records to ensure ***integrity***, usability and survivability.

A glossary of terms found in this policy is located in Appendix A - Definitions. The first occurrence of a defined term is in ***bold italics***.

2.0 Policy

2.1 Electronic information is a record if it satisfies the criteria defined by Ohio law.

2.1.1 Electronic records are compilations of ***data*** that are created or received by an agency or agency employee during the course of official duties and that document the organization, functions, policies, procedures, operations, or other activities of the office, as defined by ORC 149.011.

2.1.2 In an electronic environment, records may exist in structures other than that of familiar documents traditionally found in paper record-keeping systems.

2.1.3 Electronic records may be ***public records*** as defined by ORC 149.43 and, thus, subject to the public access provisions of ORC 149.43 (B).

2.1.3.1 Certain IT and telecommunications systems and systems infrastructure records may not be subject to release. Information such as but not limited to configurations, schematics, IP addresses, systems administration, security controls, business continuity, and incident response may not constitute information subject to mandatory disclosure. Ensure “security records” and “infrastructure records” have been properly identified as required in ORC 149.433.

Office of Information Technology | 30 East Broad Street, 39th Floor | Columbus, Ohio 43215 | 614.644.6446 | State.CIO@oit.ohio.gov
Stuart R. Davis, Assistant Director/State CIO

2.1.4 Electronic records are subject to audit and legal proceedings such as discovery and subpoenas.

2.2 Electronic records should be managed effectively as part of a comprehensive records management program.

2.2.1 In accordance with ORC 149.34 (A), the "head of each state agency, office, institution, board, or commission shall...establish, maintain, and direct an active continuing program for the effective management of the records of the state agency...".

2.2.2 Employing records management procedures (i.e., scheduling systems/files to allow for the legal ***destruction*** of data) will facilitate the most cost effective use of the state's computer resources.

2.3 State agencies, boards and commissions should keep and manage their electronic records in compliance with standards, best practices and guidelines.

2.3.1 Agencies should make the fullest possible commitment to the required use of open, public, non-proprietary standards that facilitate communication between multiple systems and software.

2.3.2 American National Standards Institute or other industry-wide standards, Office of Enterprise IT Architecture and Policy-issued best practices should be used where applicable.

2.4 Work processes and tools should support the creation and management of electronic records.

2.4.1 Provision for adequate maintenance, ***disposal*** and preservation of electronic records should be built into work process and tools so that electronic records management is a routine and time-efficient activity.

2.4.1.1 If private communication accounts or privately owned portable computing devices are permitted to conduct state business, agencies shall ensure that electronic communication records documenting state business are retained in accordance with the agency's record retention schedule.

2.4.2 Appropriate descriptive data about electronic records must be captured at the time of creation. Unlike paper records, that data cannot be determined at a later date.

2.4.3 Appropriate records management principles should be an essential component in the design of new systems or the upgrading of existing systems.

2.5 Electronic records should be created and maintained in reliable and secure systems.

2.5.1 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.

2.5.2 Reliability refers to a record's authority and trustworthiness at the time of creation. To ensure reliability, agencies must establish procedures for creating official records electronically.

2.5.3 Agencies must take measures to prevent unauthorized access to electronic records.

2.5.4 Data must be captured that document the context, content and structure of electronic records. Context establishes who created the record and the transaction of which it was a part. Content is the actual data. Structure is the format of the record. Structure must be captured so that the record can be migrated into the latest generation of hardware and software as necessary.

2.6 In most cases, electronic records should be maintained in electronic form, because preserving the context and structure of and facilitating access to those records are best accomplished in the electronic environment.

2.6.1 Electronic records can be classified as system-dependent or –independent.

2.6.2 System-dependent records are records that require an electronic environment to provide meaning, context or accessibility. System-dependent records should be migrated at least every five years.

2.6.3 System-independent records are records that can exist independently of an electronic environment. System-independent records may be reformatted, with necessary metadata, into an eye-readable media.

2.7 Maintaining and providing access to electronic records over time is a shared responsibility.

2.7.1 Records managers and information technology managers of the originating agencies, the Department of Administrative Services' State Records Administrator and the State Archives of Ohio must work together to manage, preserve and provide access to electronic records.

2.7.2 ***Transferring*** all historically significant electronic records from the originating agencies to the State Archives is neither cost effective nor practically feasible. However, in cases where the State Archives does not take physical custody of electronic records, staff will provide appropriate guidance to ensure long-term accessibility and physical preservation consistent with the applicable retention schedule.

3.0 Authority

ORC 125.18

4.0 Revision History

Date	Description of Change
05/01/1999	This Policy supersedes all previously released memoranda or policies on this topic.
01/21/2005	Removed responsibility references throughout the policy. Updated to current policy format. No substantive changes were made to policy content.
10/13/2016	Incorporated content from the rescinded Ohio IT Bulletins ITB-2007.01, "Electronic Communication and Public Records," and ITB-2006.01, "Public Records Requests Concerning IT and Telecommunications Systems." Transferred policy content to a new State of Ohio Administrative Policy Template. Re-numbered policy to IT-07 to be consistent with new numbering format.
10/13/2018	Scheduled policy review.

5.0 Inquiries

Direct inquiries about electronic records to:

State Archives
Ohio History Connection
800 E. 17th Avenue
Columbus, Ohio 43211

1-614-297-2536| statearchives@ohiohistory.org

Direct inquiries about this policy to:

State IT Policy Manager
Enterprise IT Architecture & Policy
Office of Information Technology
Ohio Department of Administrative Services
30 East Broad Street, 39th Floor
Columbus, Ohio 43215

1-614-466-6930 | DAS.State.ITPolicy.Manager@das.ohio.gov

State of Ohio Administrative Policies may be found online at
www.das.ohio.gov/forStateAgencies/Policies.aspx

Appendix A - Definitions

a. Data. Coded representation of quantities, objects and actions. The word, "data" is often used interchangeably with the word, "information," in common usage and in this policy.

b. Destruction. Rendering IT-related property unusable and its data unrecoverable through shredding, incineration or other equivalent procedure.

c. Integrity. Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.[7]

d. Public Record. Any record that is kept by any public office, including, but not limited to, state, county, city, village, township and school district units. Exceptions to the public record definition are outlined in detail in Ohio Revised Code (ORC) Section 149.43.

e. Records. Records include any document, device, or item, regardless of physical form or characteristic, created or received by or coming under the jurisdiction of any public office of the state or its political subdivisions, which serves to document the organization, functions, policies, decisions, procedures, operations, or other activities of the office (ORC 149.011).

f. Transfer or Disposal of Records. All records are the property of the public office concerned and shall not be removed, destroyed, mutilated, transferred, or otherwise damaged or disposed of, in whole or in part, except as provided by law or under the rules adopted by the records commissions provided for under sections 149.38 to 149.42 of the Revised Code or under the records programs established by the boards of trustees of state-supported institutions of higher education under section 149.33 of the Revised Code. Such records shall be delivered by outgoing officials and employees to their successors and shall not be otherwise removed, transferred, or destroyed unlawfully (ORC 149.351).

[7] "NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations," U.S. Department of Commerce National Institute of Standards and Technology, April, 2013 <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>.