OhioDAS

State of Ohio Administrative Policy

No:
Information Technology
IT-05

Effective:
April 20, 2017

Issued By:

Robert Blair, Director

Disposal, Servicing and Transfer of IT Equipment

1.0 Purpose

The purpose of this policy is to mitigate risk with regard to state ***data***, ***licensed software*** and ***intellectual property***, and rechargeable batteries and other hazardous materials in the ***disposal***, servicing or transfer of state agency ***information technology (IT) equipment***.

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

Whenever a state agency relinquishes ***custody*** of IT equipment or its components, whether temporarily (e.g., lending or servicing equipment) or permanently (e.g., ***donation***, ***trade-in***, lease termination or disposal of equipment), the agency shall take reasonable measures as outlined in this policy to prevent the unauthorized release of information, unauthorized use of licensed software and intellectual property, and improper disposal of rechargeable batteries and other hazardous materials.

State agencies shall implement policies and associated procedures in compliance with this state policy as well as the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (Media Protection Family, Control Number MP-6), NIST SP 800-88, "Guidelines for Media Sanitization," and Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data", and shall ensure that employees, contractors, temporary personnel and other agents of the state adhere to those policies.

Nothing in this policy prohibits the authorized transfer of information, licensed software and intellectual property stored on transferred IT equipment.

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 **Risk Assessment**. Prior to relinquishing custody of IT equipment, agencies shall conduct a ***risk assessment*** of the information stored on such equipment, in accordance with Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework."

2.2 **Short-Term Loan**. Prior to lending IT equipment, state agencies shall secure information in a manner consistent with the findings of their risk assessment and in accordance with NIST SP 800-53 and 800-88 to prevent the unauthorized disclosure or use of the information. If the equipment contains ***sensitive*** or ***personally identifiable information***, the agency shall either ***sanitize*** the equipment or encrypt the information commensurate with the risk-assessment findings, NIST SP 800-53 and 800-88, Ohio Administrative Policy IT-14 and in accordance with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography."

2.3 **Servicing**. Prior to servicing IT equipment, where the device leaves the custody of the agency, state agencies shall secure information in a manner consistent with the findings of their risk assessment and in accordance with NIST SP 800-53 and 800-88 to prevent the unauthorized disclosure or use of the information. If the equipment contains sensitive or personally identifiable information, the agency shall either sanitize the equipment or encrypt the information commensurate with the risk-assessment findings, NIST SP 800-53 and 800-88, Ohio Administrative Policy IT-14 and in accordance with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography." Securing, sanitizing, or encrypting is not required prior to servicing if the equipment is no longer capable of being secured, sanitized or encrypted. In such cases, removal of storage media such as hard disks that contain sensitive or personally identifiable information may be appropriate, or it may be possible to sanitize the storage media in another similar and fully functional piece of IT equipment prior to releasing custody of the equipment to be serviced. If it is impossible to sanitize the malfunctioning equipment containing sensitive or personally identifiable information, then a risk assessment shall be used to determine whether the storage media must be destroyed. It is also recommended that this contingency be included in maintenance contracts.

2.3.1 Agencies may send IT equipment only to maintenance and repair service providers who have agreed in writing to:

- maintain the ***confidentiality*** of state information;
- access information only if it is necessary for maintenance or servicing purposes; and
- destroy, sanitize or return any equipment or components that are still capable of storing information, in accordance with state and agency policy.

2.4 **Disposal, Long-Term Loan, State Surplus or Other Permanent Transfer**. State agencies shall ensure that IT equipment is sanitized commensurate with the findings of their risk-assessment and in accordance with NIST SP 800-53 and 800-88 prior to either lending such equipment long-term or permanently transferring ***ownership***, such as when donating equipment, lease termination, transferring equipment to another agency,

transferring equipment to the DAS State and Federal Surplus Services, or disposing of such equipment.

2.4.1 As a minimum, state agencies shall sanitize IT equipment and computer media that is to be permanently transferred by ***overwriting*** information with meaningless data in such a way that information cannot be reasonably recovered.

2.4.2 For sensitive or personally identifiable information, the sanitation procedures that state agencies use must provide additional assurance that information cannot be recovered. More rigorous methods, such as increasing the number of overwrites or physical ***destruction*** must be used as the levels of confidentiality and risk merit.

2.4.3 Agencies may only send IT equipment to IT sanitation service providers who have agreed in writing to:

- maintain the confidentiality of state information;
- access information only if it is necessary for sanitation purposes; and
- sanitize any equipment or components capable of storing information in accordance with state and agency policy.

2.4.4 The sanitation measures taken under this section shall be appropriate to reasonably prevent the violation of software ***license*** agreements, in accordance with Ohio Administrative Policy IT-03, "Software Licensing," prior to transferring IT equipment.

2.4.5 State agencies shall dispose of IT property that contains batteries in accordance with chapter 3745-273 of the Ohio Administrative Code and the federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec. 14301, 1996). Agencies shall abide by all other state and federal mandates regarding IT property that contains hazardous materials.

2.4.6 In the event that equipment capable of ***persistent data storage*** is transferred and sanitation methods such as data overwriting are not technically feasible, agencies shall implement alternatives appropriate for the equipment to prevent the unauthorized disclosure of sensitive or personally identifiable information or shall remove and destroy the storage media.

2.4.7 Agency data owners or data custodians (refer to Ohio Administrative Policy IT-13, "Data Classification", for a definition of the data owner and data custodian roles) shall obtain and retain a certificate of destruction with the serial number, method of destruction, and date of destruction from the service provider.

2.4.7.1 The destruction of media or equipment containing Federal Tax Information (FTI) shall not only be verified by a certificate of destruction, but shall also be witnessed by a state employee.

2.5 **Other Disposal, Servicing and Transfer Requirements**. This policy is not intended to circumvent the implementation of more rigorous safeguards for the temporary or permanent transfer of IT equipment or its components that may be outlined by law, contract or other agreement. The more stringent requirements shall take precedent.

2.6 **Procedures**. If an agency has ***excess*** or ***surplus*** IT equipment, it shall work with DAS State and Federal Surplus Services to ensure that the state assets are distributed in accordance with the requirements outlined in Ohio Revised Code (ORC) Section 125.13 and Ohio Administrative Policy AM-02, "State and Federal Surplus Program".

3.0 Authority

Federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec. 14301, 1996)

ORC 125.13, 125.18; OAC 123:5-2-01, OAC Chapter 3745-273

4.0 Revision History

Date	Description of Change
08/26/2005	Original policy.
03/19/2008	Policy requirements concerning removal and destruction of storage media added to sections 2.3 and 2.4.6 of this policy.
04/18/2011	Removed reference to Ohio IT Policy ITP-B.1, "Information Security Framework." The "Interrelationship of the Information Security Framework Policy and Subpolicies," a cross-reference table showing the relationship between Ohio IT Policy ITP-B.1 and the IT security subpolicies, was also removed. Replaced with a reference to Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework."
10/13/2016	Policy definitions were updated to align with the current security standards. Transferred policy content into the new State of Ohio Administrative Policy Template. Re-numbered policy to IT-05 to be consistent with new format.
04/20/2017	Added requirements to comply with NIST SP 800-53, NIST SP 800-88, and Ohio Administrative Policy IT-14 and updated terminology for consistency. Also, added a reference to Ohio Administrative Policy AM-02, "State and Federal Surplus Program," which replaces DAS Directive GS-D-06, "Removal of Sensitive Information from Surplus State Property and Procedures for the Relinquishing of Custody to Excess Computer Equipment".
04/20/2020	Scheduled policy review.

5.0 Inquiries

Direct inquiries about excess or surplus IT equipment to:

State and Federal Surplus Services
General Services Division

Ohio Department of Administrative Services
4200 Surface Road
Columbus, Ohio 43228

614-466-6585 | Amy.Rice@das.ohio.gov

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

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. Confidentiality. Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.[1]

b. Custody. In the context of this policy, the responsibility of control of a device through ownership, acceptance on loan, or a service agreement.

c. 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.

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

e. Disposal. The final transfer of ownership or custody of an information technology device.

f. Donation. Transferring ownership and custody of IT-related property to another entity through a gift program, grant program, or their equivalent.

g. Excess. In the context of this policy, excess refers to any IT equipment that has a remaining useful life, but is no longer needed by the agency that possesses it.

[1] "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>.

h. Information Technology (IT) Equipment: For the purposes of this policy, any information technology equipment, such as computer hardware; telecommunications equipment; digital devices such as digital copiers and facsimile machines; mobile computing devices; operational technology (e.g., building and manufacturing controls); or Internet of Things (IoT) devices that are capable of persistent data storage.

i. Intellectual Property. Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.[2]

j. License. A contract that authorizes access to software and information and outlines rights regarding the use, distribution, performance, modification, or reproduction of software and information.

k. Licensed Software. Software in any form, whether commercial, proprietary, or gratuitous, that is provided by the intellectual property holder under terms of a contract that governs use, copying, modification and distribution.

l. Overwriting. A software process that replaces data previously stored on storage media with a predetermined set of meaningless data or random patterns.[3]

m. Ownership. The responsibilities of owning a device, which includes, but is not limited to, the data risks associated with devices capable of persistent data storage.

n. Persistent Data Storage. The ability of a device to store data that is recoverable beyond a complete power cycle.

o. Personally Identifiable Information (PII). "Personally identifiable information" is information that can be used directly or in combination with other information to identify a particular individual. It includes:

- a name, identifying number, symbol, or other identifier assigned to a person,
- any information that describes anything about a person,
- any information that indicates actions done by or to a person,
- any information that indicates that a person possesses certain personal characteristics.

p. Risk Assessment. The process of identifying, prioritizing, and estimating risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.[4]

---

[2] Kuhn, D. Richard, Vincent C. Hu, W. Timothy Polk, and Shu-Jen Chang. "NIST Special Publication 800-32, Introduction to Public Key Technology and the Federal PKI Infrastructure," U.S. Department of Commerce National Institute of Standards and Technology, 26 February 2001 <http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-32.pdf >.

[3] "CNSS Instruction No. 4009, National Information Assurance (IA) Glossary," Committee on National Security Systems, 26 April 2010 <https://www.ncsc.gov/nittf/docs/CNSSI-4009_National_Information_Assurance.pdf>.

[4] "NIST Special Publication 800-53 Revision 4, "Security and Privacy Controls for Federal Information Systems

q. Sanitize. A general term referring to the actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.[5]

r. Sensitive Data. Sensitive data is any type of computerized data that presents a high or moderate degree of risk if released or disclosed without authorization. There is a high degree of risk when unauthorized release or disclosure is contrary to a legally mandated confidentiality requirement. There may be a moderate risk and potentially a high risk in cases of information for which an agency has discretion under the law to release data, particularly when the release must be made only according to agency policy or procedure. The computerized data may be certain types of personally identifiable information that is also sensitive such as medical information, social security numbers, and financial account numbers. The computerized data may also be other types of information not associated with a particular individual such as security and infrastructure records, trade secrets and business bank account information.

s. Surplus. In the context of this policy, surplus refers to any IT equipment that is no longer of use to the state. The IT equipment has completed its useful life cycle.

t. Trade-in. Transferring ownership and custody of an electronic device to a vendor through a procurement incentive program.

Appendix B - Resources

Document Name
Ohio Administrative Policy AM-02, "State and Federal Surplus Program" State of Ohio Administrative Policies
Ohio Administrative Policy IT-14, "Data Encryption and Securing Sensitive Data" State of Ohio Administrative Policies
NIST SP 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations" (Media Protection Family, Control Number MP-6) http://csrc.nist.gov/publications/PubsSPs.html
NIST Special Publication 800-88, Guidelines for Media Sanitization http://csrc.nist.gov/publications/PubsSPs.html
United States. Department of Defense. *National Industrial Security Program Operating Manual 5220.22-M*. February 2006. http://www.fas.org/sgp/library/nispom.htm
Ohio Administrative Code Chapter 3745-273. *Management Standards for Universal Waste*. http://codes.ohio.gov/oac/3745-273
Ohio Revised Code (ORC) section 125.13 and rule 123:5-2-01 of Ohio Administrative Code (OAC), Disposal of Excess and Surplus Supplies. ORC 125.13: http://codes.ohio.gov/orc/125.13 OAC 123:5-2-01: http://codes.ohio.gov/oac/123%3A5-2-01

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>.

[5] *Ibid*.

The Federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec. 14301, 1996). https://www.epa.gov/mercury/mercury-batteries