

<h2>State of Ohio IT Policy</h2> <p>Disposal, Servicing and Transfer of IT Equipment</p>	<b>No:</b>  <b>ITP-E.1</b>
	<b>Effective:</b>  <b>03/19/2008</b>
	<b>Issued By:</b> R. Steve Edmonson Director, Office of Information Technology State Chief Information Officer <b>Published By:</b> Statewide IT Policy Investment and Governance Division <b>Original Publication Date:</b> 08/26/2005

### 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.

### 2.0 Scope

Pursuant to Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," this state policy applies to every organized body, office, or agency established by the laws of the state for the exercise of any function of state government except for those specifically exempted.

The scope of this information technology policy includes state computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the state who use and administer such systems.

### 3.0 Background

In the lifecycle of IT equipment, there comes a time when an agency will relinquish **custody**. The transfer of custody may be temporary, such as when equipment is serviced or loaned. The transfer may be permanent, such as a **donation, trade-in**, lease termination or disposal through the Department of Administrative Services' (DAS) State and Federal **Surplus** Program.

Any transfer of custody of equipment poses a risk that the information, licensed software and intellectual property stored on that equipment will be transferred, too, presenting the potential of unauthorized disclosure or use. In many cases, information that appears to

have been removed may be easily recoverable. The terms of **licenses** for software and intellectual property typically carry restrictions on use and **ownership** that must be considered when relinquishing control of equipment.

In addition, there is a risk of violating state and federal regulations by improperly disposing of IT-related hazardous materials. Of chief concern is the proper disposal of rechargeable batteries, such as those found in notebook computers, mobile telephones and personal digital assistants. The federal Environmental Protection Agency provides guidelines for the disposal of batteries in accordance with the federal Mercury-Containing and Rechargeable Battery Management Act.

#### 4.0 References

- 4.1 Ohio IT Policy ITP-A.1, "Authority of the State Chief Information Officer to Establish Policy Regarding the Acquisition and Use of Computer and Telecommunications Products and Services," defines the authority of the state chief information officer to establish State of Ohio IT policies as they relate to state agencies' acquisition and use of information technology, including, but not limited to, hardware, software, technology services and security.
- 4.2 Ohio IT Policy ITP-A.26, "Software Licensing," provides policy requirements designed to address software copyright compliance issues.
- 4.3 Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," defines minimal requirements for the encryption of sensitive data within state government.
- 4.4 Ohio IT Standard ITS-SEC-02, "Enterprise Security Controls Framework," establishes the National Institute of Standards and Technology (NIST) Special Publication 800-53 as Ohio's framework for information security controls. ITS-SEC-02 also defines "enterprise controls," which are IT security controls that were selected by the state chief information officer, the chief information security officer (CISO), and the CISO Leadership Committee to establish a prioritized IT security baseline for Ohio agencies. The enterprise controls are a representation of all of the top 20 Consensus Audit Guidelines or CAG, published by the SANS Institute, and select NIST Special Publication 800-53 controls that will help defend against currently known high-priority attacks as well as those that are anticipated in the near future.
- 4.5 Chapter 3745-273 of the Ohio Administrative Code outlines the management standards for universal waste. For the purposes of this policy, agencies shall review the portions of code that apply to battery waste management standards.
- 4.6 DAS Directive GS-D-06 outlines basic procedures that require state agencies sending items to the DAS State and Federal Surplus Program to take certain steps to ensure that sensitive information and licensed material has been removed.

- 4.7 Ohio Revised Code section 125.13 and rule 123:5-2-01 of the Ohio Administrative Code, outline the requirements for disposal of excess and/or surplus supplies.
- 4.8 The federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec. 14301, 1996) contains restrictions as to the disposal of batteries.
- 4.9 A glossary of terms found in this policy is located in section 9.0 - Definitions. The first occurrence of a defined term is in ***bold italics***.

## 5.0 Policy

Whenever a state agency relinquishes custody of IT equipment or its components, whether to lend, donate, service or dispose of the 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 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.

- 5.1 **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."
- 5.2 **Short-Term Loan**. Prior to lending IT equipment, state agencies shall secure information in a manner consistent with the findings of their risk assessment to prevent the unauthorized disclosure or use of the information. If the equipment contains confidential or high-risk information, the agency shall either **sanitize** the equipment or encrypt the information commensurate with the risk-assessment findings and in accordance with Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography."
- 5.3 **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 to prevent the unauthorized disclosure or use of the information. If the equipment contains confidential or high-risk information, the agency shall either sanitize the equipment or encrypt the information commensurate with the risk-assessment findings 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 contained confidential

or high-risk data 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.

5.3.1 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 agency policy.

5.4 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 prior to either lending such equipment long-term or permanently transferring ownership, such as when donating equipment, transferring equipment to another agency, transferring equipment to the DAS State and Federal Surplus Program, or disposing of such equipment.

5.4.1 State agencies must at a minimum 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.

5.4.2 For confidential or other high-risk 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, **degaussing**, or physical **destruction** must be used as the levels of confidentiality and risk merit.

5.4.3 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 agency policy.

5.4.4 The sanitation measures taken under this section shall be appropriate to reasonably prevent the violation of software license agreements, in accordance with Ohio IT Policy ITP-A.26, "Software Licensing," prior to transferring IT equipment.

5.4.5 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.

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

**6.0 Procedures**

None.

**7.0 Implementation**

The requirements of this policy are anticipated to already be established and in practice. The policy has not been substantively revised since March of 2008.

**8.0 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 5.3 and 5.4.6 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."
03/19/2013	Scheduled policy review.

**9.0 Definitions**

- 9.1 Confidentiality. The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic customer information, patient records, information about a pending criminal case, or infrastructure specifications. Information systems that must ensure confidentiality will likely deploy techniques such as passwords, and could possibly include encryption.

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

- 9.3 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.
- 9.4 Degaussing (i.e., demagnetizing). A procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.
- 9.5 Destruction. Rendering IT-related property unusable and its data unrecoverable through shredding, incineration or other equivalent procedure.
- 9.6 Disposal. The final transfer of ownership or custody of an information technology device.
- 9.7 Donation. Transferring ownership and custody of IT-related property to another entity through a gift program, grant program, or their equivalent.
- 9.8 Intellectual Property. A commercially valuable product of the human intellect in a concrete or abstract form, such as a copyrightable work, a protectable trademark, a patentable invention, or a trade secret.<sup>1</sup>
- 9.9 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.
- 9.10 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.
- 9.11 Overwriting. Process of writing patterns of data on top of the data stored on a magnetic medium.
- 9.12 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.
- 9.13 Persistent Data Storage. The ability of a device to store data that is recoverable beyond a complete power cycle.
- 9.14 Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security.

---

<sup>1</sup> "Intellectual Property," Def. 2, Black's Law Dictionary, 7th Edition, 1999.

- 9.15 Sanitize. To expunge data from IT equipment so that data recovery is reasonably prohibitive. Sanitizing includes such measures as overwriting, degaussing and destruction.
- 9.16 Surplus. In the context of this policy, excess information technology property that state agencies send to the DAS State and Federal Surplus Program for destruction, donation, recommission or surplus sale programs.
- 9.17 Trade-in. Transferring ownership and custody of an electronic device to a vendor through a procurement incentive program.

## 10.0 Related Resources

Document Name
United States. Department of Defense. <u>National Industrial Security Program Operating Manual 5220.22-M</u> . February 2006. <a href="http://www.fas.org/sgp/library/nispom.htm">http://www.fas.org/sgp/library/nispom.htm</a>
Ohio Administrative Code Chapter 3745-273. <u>Management Standards for Universal Waste</u> . <a href="http://codes.ohio.gov/oac/3745-273">http://codes.ohio.gov/oac/3745-273</a>
Department of Administrative Services. <u>DAS Directive GS-D-06</u> . September 2009. <a href="http://das.ohio.gov/LinkClick.aspx?fileticket=yWq8Ms0xjz8%3d&amp;tabid=356">http://das.ohio.gov/LinkClick.aspx?fileticket=yWq8Ms0xjz8%3d&amp;tabid=356</a>
Ohio Revised Code section 125.13 and rule 123:5-2-01 of Ohio Administrative Code, <u>Disposal of Excess and Surplus Supplies</u> . <a href="http://codes.ohio.gov/orc/125.13">http://codes.ohio.gov/orc/125.13</a>
The federal Mercury-Containing and Rechargeable Battery Management Act (42 USC Sec. 14301, 1996). <a href="http://www.epa.gov/epaoswer/hazwaste/state/policy/pl104.pdf">http://www.epa.gov/epaoswer/hazwaste/state/policy/pl104.pdf</a>

## 11.0 Inquiries

Direct inquiries about surplus property to:

State and Federal Surplus Program  
General Services Division  
Ohio Department of Administrative Services  
4200 Surface Road  
Columbus, Ohio 43228

Telephone: 614-466-6570  
Facsimile: 614-466-6585  
E-mail: [David.Settle mire@das.state.oh.us](mailto:David.Settle mire@das.state.oh.us)

Direct inquiries about this policy to:

Enterprise IT Architecture & Policy  
Investment and Governance Division  
Ohio Office of Information Technology  
30 East Broad Street, 39<sup>th</sup> Floor

STATE OF OHIO IT POLICY  
DISPOSAL, SERVICING AND TRANSFER OF IT EQUIPMENT

Columbus, Ohio 43215

Telephone: 614-644-9352

Facsimile: 614-644-9152

E-mail: [State.ITPolicy.Manager@oit.ohio.gov](mailto:State.ITPolicy.Manager@oit.ohio.gov)

Ohio IT Policy can be found on the Internet at [www.ohio.gov/itp](http://www.ohio.gov/itp).

**12.0 Attachments**

None.