CPTC Procedure: Data Destruction and Sanitization

Coastal Pines Technical College (CPTC) regularly stores sensitive information on computer hard drives, removable media, and other forms of electronic media as well as physical media such as paper documents. Data should be stored until it reaches the end of its retention period (per the State of Georgia and TCSG retention periods) or until the equipment storing the data is no longer needed.

As new equipment is obtained and older equipment and media reach end of life, sensitive information on surplus equipment and media must be properly destroyed and otherwise made unreadable to protect confidential information or personally identifiable information (PII). TCSG refers to this as “information not for public dissemination” in the Information Security Standards.

Proper disposal and disposition of surplus computer hardware and other storage media manages risks of security breach and inappropriate information disclosure. This procedure is designed to address proper disposal procedures for any media that stores or has stored confidential information and/or PII. Proper sanitization and disposal procedures are critical to ensuring data privacy and license compliance.

Procedure:

The transfer or disposition of data processing equipment, such as computers and related media, shall be controlled and managed according to O.C.G.A. § 10-15-2 guidelines. Data remains present on any type of storage device (whether fixed or removable) even after a disc is “formatted”, power is removed, and the device is decommissioned. Simply deleting the data and formatting the disk does not prevent individuals from restoring data. Sanitization of the media removes information in such a way that data recovery using common techniques or analysis is greatly reduced or prevented.

All documentation, hardware, and storage that have been used to process, store, or transmit confidential information or PII shall not be released into general surplus until it has been sanitized and all stored information has been cleared using an approved method. Further information is available in TCSG’s Information Security Standards.

Data Disposal Procedures

The DOAS Georgia Surplus Property Manual addresses disposal of equipment. Disposal Authorization is outlined in chapter 13. All computer desktops, laptops, hard drives, and portable media destined for disposal must be processed through Administrative Services via Inventory Transfer Forms for proper disposal. In section 14.5, the manual states that:

> *Surplus has an agency contract for the disposal of all electronic equipment. The contract requires that all disposals conform to US Environmental Protection Agency (EPA) regulations and that all data storage devices are destroyed in a way data is unrecoverable. Essentially, all electronics are de-manufactured (shredded) to their base components (plastic, metal, glass, etc.) that are then recycled. Use of the DOAS contract is mandatory.*

The manual also states that:

> *Affidavit of Disposal is not required if ELC # is provided.*

The Executive Director of Information Technology or designee approves all such disposals before they are processed. Paper and hard copy records with PII shall be disposed of in a secure manner as to render the information irretrievable. Such disposal shall be conducted by personnel who are authorized to dispose of sensitive information or equipment. Procedures to make the information irretrievable may include shredding or incinerating of hard copy materials so that sensitive information cannot be reconstructed. Approved disposal methods include the following.

Electronic Media (physical hard drives, tape cartridge, CDs/DVDs, flash drives, printer and copier hard-drives, etc.) shall be disposed of by one of the following methods:

- *CDs/DVDs with sensitive information will be destroyed in a shredder or sent to surplus;*
- *If the useful life of the device is over, the custodian shall send the item to surplus or eScrap. When the device is transferred to eScrap, the state contractor essentially gives the state a certificate of destruction and becomes responsible for any leaked PII that occurred after transfer;*
- *Overwriting Magnetic Media – overwriting uses an approved program to write binary data sector by sector onto the media that requires sanitization; and*
- *Physical Destruction – implies complete destruction of media by means of crushing or disassembling the asset and ensuring no data can be extracted or recreated from the remaining materials.*

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this procedure. Examples of documentation include:

- On-demand documented procedures related to surplus disposal of hardware and software;
- Data destruction and surplus logs of equipment identified for disposal; and
- Physical evidence of sanitized assets and/or data destruction/cleansing devices, software, and procedures

Responsibility

The Executive Director of Information Technology has the overall responsibility for ensuring this procedure is implemented.

Adopted: February 14, 2019
Revised: September 19, 2023

Appendix: Supporting Documentation

§ 10-15-2. Disposal of business records containing personal information
A business may not discard a record containing personal information unless it:

1. *Shreds the customer's record before discarding the record;*
2. *Erases the personal information contained in the customer's record before discarding the record;*
3. *Modifies the customer's record to make the personal information unreadable before discarding the record; or*
4. *Takes actions that it reasonably believes will ensure that no unauthorized person will have access to the personal information contained in the customer's record for the period between the record's disposal and the record's destruction.*

§ 10-15-6. Penalty; hearing; effect of judgment

A. *If the Attorney General determines, after notice and hearing, that a business has violated Code Section 10-15-2, the Attorney General may issue an administrative order imposing a penalty of not more than $500.00 for each customer's record that contains personal information that is wrongfully disposed of or discarded; provided, however, in no event shall the total fine levied by the Attorney General exceed $10,000.00. It shall be an affirmative defense to the wrongful disposing of or discarding of a customer's record that contains personal information if the business can show that it used due diligence in its attempt to properly dispose of or discard such records.*
B. *If the Attorney General determines, after notice and hearing, that a business has violated Code Section 10-15-3, the Attorney General may issue an administrative order imposing a penalty of not more than $250.00 for the first violation of Code Section 10-15-3, and a penalty of $1,000.00 for a second or subsequent violation of Code Section 10-15-3.*
C. *The hearing and any administrative review in connection with alleged violations of Code Section 10-15-2 or 10-15-3 shall be conducted in accordance with the procedure for contested cases pursuant to Chapter 13 of Title 50, the "Georgia Administrative Procedure Act." Any person who has exhausted all administrative remedies available and who is aggrieved or adversely affected by a final order or action of the Attorney General shall have the right of judicial review in accordance with Chapter 13 of Title 50, the "Georgia Administrative Procedure Act."*
D. *The Attorney General may file in the superior court of the county in which the person under an order resides, or if the person is a corporation, in the superior court of the county in which the corporation under an order maintains its principal place of business, a certified copy of or the final order of the Attorney General, whether or not the order was appealed. Thereafter the court shall render a judgment in accordance with the order and notify the parties. The judgment shall have the same effect as a judgment rendered by the court.*