



Office of the
Washington
State Auditor
Pat McCarthy

PERFORMANCE AUDIT

Report Highlights

Safe Data Disposal at a College

Like most state agencies, public institutions of higher education (see sidebar) have the authority to dispose of all the equipment they no longer need for their operations. Their surplus programs take unwanted property – including information technology (IT) equipment like computers, cell phones and printers – and resell, recycle or otherwise dispose of it.

However, colleges handle many records that contain confidential information, including student identification and Social Security numbers or personal banking and medical information. State law requires them to destroy or arrange for the destruction of such data before they can send the IT equipment that stored it to surplus. Releasing such information can harm a person's privacy and financial security, and pose the risk of identity theft.

To help colleges and other agencies comply with the law, Washington Technology Solutions (WaTech) developed the Media Sanitization and Disposal Standard. Following the standard helps ensure that discarded data-handling media – meaning any portion of a device that can store or process data – is securely sanitized using one of three sanitizing methods: clearing, purging or destruction, depending on the data category that is stored in the media.

Our Office has conducted two audits evaluating how well state agencies, including a few colleges, removed confidential data from IT devices before selling them through the Department of Enterprise Services (DES) surplus program. This audit sought to evaluate how surplus IT equipment was handled in a higher education setting that does not participate in the DES program but uses its own procedures.

This report used the term “colleges” to indicate both types of institutions of higher education: colleges and universities.

It also did not disclose detailed results of individual tests we performed to decrease the risk to the audited college's data security. As an added precaution, we also did not disclose the identity of the college we audited.

The college has adopted a strong process and had properly sanitized all the IT equipment we tested

The college's process for sanitizing IT equipment has several strengths worth highlighting. For example, the college:

- Only resells IT equipment that can be sanitized
- Treats every device as if it contains confidential information
- Uses professional sanitization systems to sanitize devices

Having a strict approach to media sanitization provides assurance no confidential information remains in the equipment prepared for surplus. To have a policy less strict presents a greater risk of a data breach, should one poorly prepared device fall into the wrong hands.

All surplus IT equipment we tested at the college was properly sanitized: we did not find any confidential data on the tested devices. Because our sample was not truly random, we cannot statistically project our results to all equipment at the college. Nonetheless, given the strong process the college has in place, plus the fact that all the devices we tested were properly sanitized, we are confident that the college has a good process in place to consistently sanitize its IT equipment. Additionally, to obtain the necessary assurance that its sanitizing procedures are working as intended, the college verifies some of its results through testing. However, to help ensure procedures remain successful, the college should test a greater proportion of sanitized IT equipment.

State Auditor's Conclusions

The results of this audit reflect the important progress Washington state government has made in addressing the risks associated with disposing of computers and other information technology (IT) equipment that may contain confidential data. In our first audit of data disposal in 2014, we estimated 9% of state computers scheduled for sale during our review period contained confidential data that should have been removed. This audit looked at how a college that does not participate in the state's centralized surplus program handled IT equipment. We found commendable levels of security and efficiency.

Colleges and universities possess tremendous amounts of confidential data, including personal information for each of their students, making safe data disposal imperative. The college we reviewed assumes every surplus machine contains confidential information and acts accordingly. The college purchased industrial-grade equipment to sanitize surplus hard drives. And its policy calls for physically destroying a drive if staff encounter any difficulties in erasing its data.

We tested a sample of IT equipment in the college's surplus program, and none contained confidential data. We are confident that the process in place is a good one. We do make a recommendation to help improve the college's process. As with every undertaking in government, safely disposing of technology requires a vigilant commitment to improvement. Through that commitment, we better protect the information of everyone who relies on public services.

Recommendations

We made a recommendation to the college to improve its verification process of media sanitization results. In developing the process, we recommended the college consults with WaTech to determine the appropriate volume and frequency of testing.