

# ITAD - Don't Forget the Process

## Considerations for Developing an IT Disposal Policy

Disposal of an IT asset is the last set of activities in the lifecycle; a process area for which few give much thought. I mean, what is there to ponder? The IT asset in question is no longer needed by your organization – so get rid of it! Ah, but the adage “one man’s trash is another man’s treasure” certainly applies. Just because a piece of technology has outlived its usefulness for your internal customers doesn’t mean the asset has no value, regardless of age or operational condition. And, not every IT asset being returned is owned by your organization, such as leased equipment.

In all cases though, an aspect of security must be addressed. These days, most technology has some form of data storage which must be thoroughly cleansed, or even removed and destroyed, in order to ensure that no proprietary, personal or other sensitive information is released outside of your organizational control.

Lastly, there are growing global concerns about the environmental impact related to disposal of electronic devices in general; not just the space they take up in a land fill, but heavy metals leaching into water supplies, recycling of components and source materials to conserve resources, etc. So much so that many governments have enacted laws mandating adherence to e-waste controls for manufacturing and disposal.

So, where to begin?

### Scope Considerations

The scope of the disposal activities must be explicitly defined in the policy. Does the policy encompass all technology? Will it address full systems only or include subsystems and components? Physical location must also be tracked.

Further, will the policy apply to technology not owned by the organization, such as that owned and used by contracted 3<sup>rd</sup>-parties for the purposes of conducting the business and processing data of the organization? This is particularly important when considering data security concerns for technology prior to removal from service or physically the organization’s office locations.

To improve understanding, it’s recommended that technology in scope be listed in the policy. For example:

- Desktop and laptop computers
- Computer servers and server arrays
- Special purpose “appliances” (typically represented by a combination of server hardware and software, purchased

together as a single, preconfigured product)

- Network equipment
- Storage devices and subsystems
- Networked printers and multi-function printing devices
- Licensed software products
- Computer peripherals
- Computer components

The other consideration for scope is geographic coverage. Most organizational disposal policies are written to be enterprise-wide (i.e. “global” in nature) with location-specific issues called out as exceptions. Facility ownership is another aspect of location coverage, with the policy written to apply to all locations where organizational technology assets are operated, stored or otherwise managed, regardless of whether that location is directly managed by the organization or a contracted 3<sup>rd</sup>-party.

### Considerations for Assignment of Responsibility

Since it pertains to technology, it is typical to assign responsibility for management and execution of IT asset disposal to the Information Technology (IT) group as part of technology operations and service delivery. The defined responsibility must provide for continuous oversight of the technology disposal program, processes and records, regardless of the parties delivering the execution of physical technology disposal activities and tasks.

It is important to note that this last point speaks to the growing practice by organizations of all sizes, industries and national origin to outsource the actual IT asset disposal services. This is largely due to increasing regulatory pressures and e-waste requirements, all of which becomes even more complex and challenging for geographically diverse organizations given the lack of standards across governmental boundaries.

### Identifying and Addressing Applicable Laws and Regulations

There are many factors that can influence the disposal of technology, but of utmost concern are compliance with the laws and regulations governing our industry, sound financial management, and thoughtful consideration for the communities in which we conduct business by considering environmental impact.

The disposal of technology must meet applicable governmental laws in all jurisdictions and industry



regulations, including, but not limited to:

- All environmental laws regulating waste
- All laws controlling copyright infringement specific to licensed software
- All laws and industry regulations regarding protection of sensitive data
- All industry regulations regarding accurate tracking of technology inventory

The potential for corporate espionage from old computers is significant. If a discarded computer with an unprocessed hard drive falls into the wrong hands, they would have all the time in the world to uncover confidential company data. Typical types of proprietary corporate data that can be compromised if unknowingly distributed include client lists and contact information, financial information such as budgets, company strategic business plans, and more.

There are a number of organizations representing major software vendors primarily for enforcement of copyright infringement, including:

- Business Software Alliance (BSA) – [www.bsa.org](http://www.bsa.org)
- Canadian Alliance Against Software Theft (CAAST) – [www.caast.com](http://www.caast.com)
- Software & Information Industry Association (SIIA) – [www.sii.net](http://www.sii.net)
- Federation Against Software Theft (FAST) – [www.fast.org.uk](http://www.fast.org.uk)

While they have many functions, these associations, in the past few years have embarked on aggressive anti-piracy programs. Actively seeking out and prosecuting companies of all sizes and industries when any evidence of improper software license management can be found, the fines levied can be significant.

As a subordinate responsibility of Financial Management, all

organizations must strive to maximize the derived benefits of technology investments including evaluation and recovery of reasonable residual value of assets deemed to no longer serve their needs.

### Determination of Residual Value

Before any owned technology is disposed, determination of residual value must be accomplished. Given the considerable diversity of available technologies, the distributed nature of the IT support organization and geographic considerations, it may be advisable to not define specific methods or criteria for determination of residual value, but instead direct the IT group together with Finance and the Line of Businesses (LOB) or Business Units (BU) to establish appropriate measures and controls.

### Disposal Methods

Technology disposal practices that are efficient with regard to physical storage of technology assets no longer in use must be adopted and exercised. There are three primary methods of disposal:

- **Transfer of Ownership** - The sale of non-hazardous, working technology should be the preferred disposal method whenever the residual value of the technology is determined to exceed the administrative and operational costs associated with this method of disposal. All retired software should be sold whenever possible, in accordance with manufacturer end-user license agreements and applicable copyright law. The donation of non-hazardous, working technology to a verified charitable organization may be considered on a case by case basis; approval must be required by an authorized manager with financial authority equal to or exceeding the residual value of the technology. The donation of retired software, whether together with associated hardware or independently, to a verified charitable organization may be considered on a case by case basis but only in accordance with manufacturer end-user license agreements and applicable copyright law; approval must be required by an authorized manager with financial authority equal to or exceeding the residual value of the technology.
- **Component Recovery** - Technology assets should be salvaged for recovery of individual components whenever this approach is determined to support current operational support practices and be cost efficient, or if likely to yield a higher value than sale of the asset as a whole. Whenever this process results in remaining unusable technology components or parts they must be physically disposed of according to the Electronic Waste Recycling provisions as defined within the overall policy.
- **Electronic Waste Recycling** - Physical destruction and disposal of unusable or hazardous technology must be handled by certified and/or licensed professionals and

disposed of according to applicable electronic waste disposal laws and guidelines.

Given the considerable diversity of available technologies, the distributed nature of most IT support groups and geographic/governmental considerations, it is common that the policy will not define specific methods or criteria for electronic waste recycling, but instead direct the organization to solicit, establish and maintain contractual relationships with appropriate, accredited vendors to support this process.

### Sanitation of Data Storage

Identity theft is one of the fastest growing crimes in America and costs consumers and businesses millions of dollars each year. Companies that don't protect the data on old computers are contributing to identity theft by leaking everything from employee and customer social security numbers to credit card accounts, retirement plans and more.

As a result, all technology hardware must be evaluated to determine whether any form of non-volatile data storage exists as part of the asset in question. The vendor provided product documentation, with product model specification, should be the primary reference.

Upon retirement of technology assets and prior to its transfer out of any form of service from the organization, all data and software must be removed from hard drives and/or the media must be destroyed, using current best practices for the type of media involved to ensure security of institutional data, user and customer privacy, and software license compliance.

There are two primary methods of electronic data storage sanitation:

- Erasure – A non-destructive means of removing data from obvious and immediate access, the Erasure method of data storage sanitation is typically used whenever the technology retains both usefulness and value to the organization and is being removed from active use for the purposes of reassignment or storage for future redeployment.

The only other situation where the Erasure method of data storage sanitation may be used is for technology not owned by the organization. In this case, it is typically not feasible (cost effective, from a contractual service perspective) for it to be stipulated that electronic data storage is removed and destroyed.

- Destruction – Complete and permanent elimination of data access, destruction of electronic data storage media is to be used whenever technology transfers ownership or is disposed through electronic waste recycling. This is because Delete, Remove, and Quick Format operating system commands, as well as disconnecting or clipping wires to a drive, do not actually erase data from the media, and therefore are not acceptable methods for preparing media for final disposal requiring permanent elimination of data access.

In support of this policy and specifically data storage sanitation, the policy should stipulate that all operational support organizations responsible for the various technologies acquired and deployed to support the



IT drives your business. So naturally, it consumes your thoughts. Customers, on the other hand, shouldn't need to think about it at all. They just expect great service. Our approach to Business Service Management helps ensure they get it, by managing IT services based on their impact to your business. That way, with your service commitments fully in sync with your business demands, you'll be able to give your customers that most coveted and elusive of all service experiences: complete satisfaction. Of course, we'll know the source of that satisfaction is really your very own IT department.

To learn more about the CA IT asset management solutions, visit <http://www.ca.com/us/information-asset-management.aspx>



organization must maintain ready access to product documentation for all technology under their management to ensure availability of the requisite procedures to erase or remove electronic data storage media.

## Record Keeping

Once retired from organizational use, the responsible internal and/or contracted disposal vendors must follow appropriate guidelines to ensure that the liability for technology hardware and software has been relinquished. Furthermore, records must be maintained attesting to the erasure of licensed software and institutional data by an approved IT service provider prior to removal of equipment from organizational facilities for any reason, including return to lessor or vendor, and completion of purchase or donation.

These guidelines should be established as part of each respective contract involved in the IT disposal process, to include but not limited to:

- Completion of necessary documentation wherever applicable, such as certificate of destruction, Bill of Sale, and receipt from electronic waste recycling facilities
- Maintain method of disposal as an attribute of inventory records
- Upon disposal, a complete stock report of the items must be given to <ORGANIZATION NAME> Finance department, detailing the following fields:
  - ◊ Item description/type of equipment (i.e., desktop computer, monitor or software title)
  - ◊ Date discarded
  - ◊ Method-of-disposal (sold/donated/recycled)
  - ◊ Purchase value
  - ◊ Date purchased
  - ◊ Goodwill value (best estimate of the worth of the individual component at time of disposal)
  - ◊ Amount of proceeds, per item (if sold)

## Reporting

Reporting of all technology disposal activity and detailed asset disposition should be conducted and made available online on a regularly scheduled basis, typically monthly.

The following are samples of what is anticipated:

- Summary of all assets scheduled to retire in days by Category and Type
- Detailed or “drill-down” reports for each asset type
- Detailed or “drill-down” reports by given date ranges. For example, all the disposed assets processed within the last 30 days; or assets that have been stored from longer than 120 days, etc.
- Summary and detailed reports for disposed assets, by Site, BU, and LOB

## References

Include citations for all external information sources, such as relevant government laws and regulations. Several applicable examples are:

- Information Technology Infrastructure Library (ITIL)
- (US) Government Information Security Reform Act (GISRA)
- General US EPA Law <http://www.epa.gov/epaoswer/hazwaste/id/univwast/index.htm>
- Federal Register, Part IV, Environmental Protection Agency, 40 CFR Part 260 et al. <http://www.epa.gov/epaoswer/hazwaste/recycle/electron/crt-fr.pdf>
- European Union WEEE Directive (2002) <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0096:EN:HTML>
- Health Canada F&DA (R.S., 1985, c. F-27) <http://laws.justice.gc.ca/en/f-27/61279.html>
- Canadian Environmental Protection Act (CEPA 99) <http://dsp-psd.pwgsc.gc.ca/Collection/H164-13-2006E.pdf>
- Ontario - Environment Protection Act Regulation 347
- Quebec - Hazardous Materials Environment Quality Act, Q-2, r.15.1
- FDA (US) 21 CFR Part 11 <http://www.21cfrpart11.com/>
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) [http://www.privcom.gc.ca/legislation/02\\_06\\_01\\_01\\_e.asp](http://www.privcom.gc.ca/legislation/02_06_01_01_e.asp)
- European Union (EU) Data Protection Directive (1998) [http://www.cdt.org/privacy/eudirective/EU\\_Directive\\_.html](http://www.cdt.org/privacy/eudirective/EU_Directive_.html)
- Sarbanes-Oxley Act <http://www.soxlaw.com/>
- Gramm-Leach-Bliley Act <http://www.ftc.gov/privacy/privacyinitiatives/glbact.html>
- Health Insurance Portability and Accountability Act (HIPAA) <http://aspe.hhs.gov/admsimp/pl104191.htm>
- Business Software Alliance (BSA) <http://www.bsa.org>
- Software & Information Industry Association (SIIA) <http://www.sii.net>
- Federation Against Software Theft (FAST) <http://www.fast.org>

In conclusion, there are quite a number of factors to consider when creating or updating an organizational IT disposal policy. The best recommendation is to spend adequate time up-front in planning the scope and impacts, soliciting input, fostering buy-in and gaining consensus.

**Howard G. Hasting**  
*Senior Principle Product Manager*  
*CA, Inc.*