

# Considerations for Developing an IT Disposal Policy

DECEMBER 2009

Howard Hastings and Shawn Sande

CA IT ASSET MANAGEMENT





---

## Table of Contents

---

<b>Executive Summary</b>	<b>1</b>
<b>SECTION 1:</b>	<b>2</b>
The Disposal “Problem”	
<b>SECTION 2:</b>	<b>2</b>
Scoping a Disposal Policy	
<b>SECTION 3:</b>	<b>3</b>
Assignment of Responsibility	
<b>SECTION 4</b>	<b>4</b>
Identifying and Addressing Applicable Laws and Regulations	
Determination of Residual Value	
Disposal Methods	
Sanitation of Data Storage	
Record Keeping	
Reporting	
<b>SECTION 5</b>	<b>7</b>
Policy References	
<b>SECTION 6</b>	<b>8</b>
Conclusions	
<b>SECTION 7</b>	<b>9</b>
About the Authors	



# Executive Summary

## Challenge

Disposal is the final chapter in the IT asset management story, but it is rarely cause for celebration. Hundreds of millions of unserviceable or decommissioned technology assets sit idle worldwide, posing a significant challenge to IT professionals. Should they refurbish, sell, donate, or dispose of these IT assets? And what are the consequences if these activities go awry? At the same time, organizations must contend with tracking these lifecycle events to maintain a complete audit trail. The disposal “problem” is as much about managing the intangible—risk—as it is about managing the tangible—obsolete inventory. Organizations lacking a unified approach to disposal will find it increasingly difficult to guard against the ecological, regulatory, legal, and financial repercussions of improperly disposing of technology assets.

## Opportunity

A formal disposal policy provides a forum for organizations to explicitly define their disposal activities, geographic reaches, roles and responsibilities, and execution and record-keeping requirements. This policy enables organizations to coordinate complex international laws and industry regulations, accounting rules, and sanitation and disposal options so that they can properly remove technology assets from their inventory rolls and minimize their risk profile.

## Benefits

Scoping, developing, and implementing a comprehensive IT asset disposal policy helps organizations properly close the loop on the IT asset lifecycle while confidently:

- Mitigating legal and financial risks posed by regulatory noncompliance
- Safeguarding sensitive data and reducing security risks posed by improper data storage sanitation
- Reducing software license liabilities and the likelihood of software audits
- Maintaining complete disposal records, including disposition and financial data
- Demonstrating green leadership by disposing of technology assets in an ecologically sound manner



## The Disposal “Problem”

Disposal marks the end of the IT asset lifecycle, but little thought is devoted to disposal processes. Many organizations address the disposal “problem” myopically. When an IT asset is no longer of any use, they simply get rid of it. But just because a piece of technology has outlived its use for your internal customers does not mean it is of less value, regardless of age or operational condition. What is more, not every returned IT asset is owned by your organization (e.g. leased equipment). Developing a strategy for physically disposing of IT assets at the end of their useful life is just the first of many important considerations.

You also have to contend with security issues. Most modern technology devices include some form of physical data storage that must be thoroughly sanitized, removed, or destroyed before disposal to protect proprietary, personal, or other sensitive data.


Lastly, environmental considerations increasingly govern how and where electronic devices are finally disposed. When they are successful, recycling efforts can reclaim valuable resources for post-consumer reuse. But far too often, electronic devices end up in massive landfills where they leach non-biodegradable and toxic materials into the soil, groundwater, and even the air. This has prompted numerous governments to enact statutes mandating electronic waste (e-waste) controls in both manufacturing and disposal processes.

The disposal problem is multifaceted and begs several important questions: Should you refurbish, sell, donate, return, or dispose? How should you approach security? What are the regulatory and environmental consequences of your disposal program? Where do you begin?

## Scoping a Disposal Policy

Scoping and documenting your disposal policy is a logical place to begin, but beware: the disposal activities comprising your policy must be explicitly defined. First, consider the following questions:

- Does the policy encompass all of your technology?
- Does the policy exclusively address complete systems, or does it also incorporate subsystems and components?
- Will the policy apply to technology that you do not own, such as technology owned and operated by contracted third parties who conduct business and process data on your behalf? (This is an important data security consideration when decommissioning and removing assets from the premises.)



You should also identify the physical location and type of technology the policy covers, including:

- Desktop and laptop computers
- Computer servers and server arrays
- Special purpose “appliances” (e.g. a combination of server hardware and software purchased as a single, preconfigured product)
- Network equipment
- Storage devices and subsystems
- Networked printers and multi-function printing devices
- Computer peripherals
- Computer components
- Software installation materials, documentation, and license certificates

Finally, do not neglect to consider geographic coverage in your policy. Organizations typically draft enterprise-wide or global disposal policies, and these policies should be capable of accommodating location-specific information as exceptions. But facility assignment also factors into geographic coverage, with policies sometimes written to accommodate every location where technology assets are used, stored, or otherwise managed—regardless of whether the location is managed by the organization or a contracted third party.

## Assignment of Responsibility

Responsibility for the management and execution of IT asset disposal typically falls to an organization’s Information Technology (IT) group as a function of technology operations and service delivery. Specific responsibilities should be defined to ensure continuous oversight of the technology disposal program, processes, and records, regardless of who is physically conducting the disposal activities and tasks. This is especially important given the growing practice—among organizations of all sizes, industries, and geographies—to outsource physical IT asset disposal services. The growth of these services stems from increasing regulatory oversight and more stringent e-waste laws, which have increased the complexity of disposal practices for geographically-dispersed organizations contending with multifarious e-waste regulations.



## Identifying and Addressing Applicable Laws and Regulations

Several factors influence disposal policies, but none more so than regulatory compliance, fiduciary accountability, and environmental stewardship. Corporate citizenship plays a role in molding an organization's disposal policy to an extent, but compliance is not entirely driven by benevolence. More often, it is driven by aversion to risk. In the case of regulatory oversight, compliance is viewed as a means of mitigating legal and financial risk posed by statutes and industry regulations spanning multiple jurisdictions. These include:

- Environmental statutes regarding waste
- Statutes governing copyright infringement specific to licensed software
- Statutes and industry regulations governing the protection of sensitive data
- Industry regulations mandating the accurate tracking and management of technology products

Risk also emanates from lax security. The potential for corporate espionage from old computers is well documented. Discarded computers with un-sanitized hard drives expose organizations to considerable risk, especially when customer data or proprietary or sensitive business data (client lists, contact information, budget data, strategic business plans, etc) is lost or stolen.

Software license liabilities also pose significant risks. Several organizations now independently represent major software vendors in anti-piracy initiatives and copyright infringement cases. The most widely known of these organizations include:

- The Business Software Alliance (BSA), [www.bsa.org](http://www.bsa.org)
- The Software and Information Industry Association (SIIA), [www.siiia.net](http://www.siiia.net)
- The Federation Against Software Theft (FAST), [www.fast.org.uk](http://www.fast.org.uk)

While these organizations perform a wide array of functions, in recent years they have embarked on aggressive anti-piracy campaigns, actively seeking and prosecuting companies of any size in all industries whenever improper software license management is reported. Resulting fines and true-up efforts are typically very costly for what these organizations refer to as “target” organizations.

### Determination of Residual Value

As a subordinate responsibility of financial management, organizations must maximize the derived benefits of their technology investments, including the evaluation and recovery of the reasonable residual value of assets deemed no longer serviceable. Before disposing of any owned asset, its residual value must be ascertained. Given the considerable diversity of technology alternatives, the distributed nature of IT support organizations, and geographic considerations, codified methodologies or criteria for the determination of residual value are not generally recommended. Instead, the IT group should collaborate with the finance department and the lines of business (LOBs) or business units (BUs) to establish appropriate measures and controls.



## Disposal Methods

Operationally, organizations must contend with the physical disposition of technology assets no longer in use. There are three primary methods of disposal (note that these methods are not mutually exclusive):

1. **Transfer of Ownership** – The sale of non-hazardous, functioning technology should be the preferred method of disposal whenever the residual value of the technology exceeds the administrative and operational costs associated with its transfer. Retired software should be harvested and sold whenever possible, in accordance with manufacturers' end-user license agreements and applicable copyright laws.  
  
Donating non-hazardous, functioning technology to registered charitable organizations, non-profits, and trusts should be considered on a case-by-case basis. Likewise, donating retired software (whether independent or loaded on associated hardware) to registered charitable organizations, non-profits, and trusts should be considered on a case-by-case basis and must adhere to manufacturers' end-user license agreements and applicable copyright laws. Approval for all donations—hardware and software—should be authorized by managers possessing financial approval thresholds equal to or exceeding the residual value of the donated technology.
2. **Component Recovery** – Technology assets should be salvaged and individual components recovered when this approach conforms to existing operational support practices and is deemed cost-efficient, or when this approach is likely to yield a higher return than the sale of any given asset as a whole. Any remaining unusable technology components or parts should be physically disposed of in accordance with the Electronic Waste Recycling provisions defined in the organization's disposal policy (see below).
3. **Electronic Waste Recycling** – The physical destruction and disposal of unusable or hazardous technology should be undertaken by certified or licensed e-waste professionals; disposal practices should conform to applicable e-waste statutes and guidelines. Given the considerable diversity of technology alternatives, the distributed nature of IT support organizations and geographic considerations, it is uncommon for organizations to codify and execute e-waste recycling processes. Instead, the organization should consider soliciting, establishing, and maintaining contractual relationships with accredited third-party vendors to support the e-waste recycling process.



### Sanitation of Data Storage


Identity theft is one of the fastest growing crimes in the world, costing consumers and businesses billions of dollars each year. Organizations that fail to safeguard data on old or unserviceable computers actively contribute to the proliferation of identity theft by exposing sensitive personal data (password vaults, social security numbers, credit card numbers, bank account information, etc) to unscrupulous parties. This exposes organizations to significant risk stemming from damage to reputation, regulatory non-compliance, and class-action lawsuits.

Prevention of data theft begins with an examination of all technology assets to determine if they contain any form of non-volatile data storage. (Product model specifications can be sourced from the vendor's product documentation.) As technology assets are retired—and before they are transferred out of service—all data and software must be removed from hard drives or other physical media pursuant to media-specific best practices, lest the organization jeopardize the security of institutional data, user and customer privacy, and software license compliance. There are two primary methods of electronic data storage sanitation:

1. Erasure - A non-destructive means of purging data from obvious and immediate access that is commonly employed when technology assets retain both usefulness and value. Owned assets are typically sanitized and removed from active use pending redeployment. For assets not owned by the organization, erasure is preferred, because it is generally cost-prohibitive to contractually stipulate the removal and destruction of electronic data storage media.
2. Destruction - Complete and permanent elimination of data access that is commonly employed when disposal occurs through technology ownership transfer or e-waste recycling. Destruction is preferred here, because "Delete," "Remove," and "Quick Format" operating system instructions or physical intercession (clipping or disconnecting drive wires) do not adequately cleanse data from the media and therefore are not acceptable media preparation approaches. An organization's disposal policy should incorporate operational guidelines for media destruction, identifying the operational support groups responsible for all technologies acquired and deployed in support of the organization. A comprehensive product documentation library must also be maintained to guide electronic data storage media erasure/removal efforts.

### Record Keeping

Once a technology asset is retired from service, the responsible internal group or contracted disposal vendor must follow appropriate guidelines to ensure all liabilities for the asset are relinquished. Responsible parties must attest to the removal of licensed software and institutional data by an approved IT service provider before technology assets leave the premises; this includes equipment returned to a lessor or vendor and equipment slated for sale or donation.



These guidelines should be explicitly defined, thoroughly documented, and incorporated into every contract associated with the IT asset disposal process. Examples include:

- Completing applicable documentation, such as certificate of destruction, bill of sale, and receipt by an e-waste recycling facility
- Maintaining “Method of Disposal” as an inventory attribute
- Providing the finance department with a comprehensive stock disposal report, including—
  - Item description and type (desktop computer, monitor, software title, etc)
  - Date discarded
  - Method of disposal (soled/donated/recycled)
  - Purchase value
  - Date purchased
  - Goodwill value (best estimate of the value of the individual component at the time of disposal)
  - Amount of proceeds per item (if sold)

### Reporting

Detailed reporting of disposal activity and asset disposition should be conducted and published online on a regularly scheduled basis, typically monthly. At a minimum, you should consider:

- A summary asset retirement timeline by asset category and asset type
- Detailed, drill-down reports for each asset type
- Detailed, drill-down reports by date range (e.g. “Show me all disposed assets for the past 30 days” or “Show me all assets in storage greater than 120 days”)
- Summary and detailed reports for disposed assets by location, business unit, or line of business

### Policy References

When drafting your organization’s disposal policy, be certain to include citations for external source material, such as relevant government statutes or industry best practices. Notable sources include:

- Australian Privacy Laws — <http://www.privacy.gov.au/law/states>
- The Basel Convention (International treaty designed to reduce the movements of hazardous waste between nations, and specifically to prevent transfer of hazardous waste from developed to less developed countries.) — <http://www.basel.int>
- Business Software Alliance (BSA) — <http://www.bsa.org>
- Canadian Environmental Protection Act (CEPA 99) — <http://dsp-psd.pwgsc.gc.ca/Collection/H164-13-2006E.pdf>
- Canadian Personal Information Protection and Electronic Documents Act (PIPEDA) — [http://www.priv.gc.ca/legislation/02\\_06\\_01\\_e.cfm](http://www.priv.gc.ca/legislation/02_06_01_e.cfm)

- Environmental Protection Agency (EPA) Regulations — <http://www.epa.gov/waste/conserve/materials/ecycling/rules.htm>
- European Union (EU) Data Protection Directive (1998) — [http://ec.europa.eu/justice\\_home/fsj/privacy/](http://ec.europa.eu/justice_home/fsj/privacy/)
- European Union WEEE Directive (2002) — <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0096:EN:HTML>
- FDA 21 CFR Part 11 — <http://www.21cfrpart11.com/>
- Federation Against Software Theft (FAST) — <http://www.fast.org>
- Government Information Security Reform Act (GISRA)
- 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>
- Information Technology Infrastructure Library (ITIL)
- International Anti-piracy Law and Copyright Laws — [http://www.sharewarejustice.com/software\\_copyright\\_law.htm](http://www.sharewarejustice.com/software_copyright_law.htm)
- Ontario Environment Protection Act Regulation 347
- Quebec Hazardous Materials Environment Quality Act, Q-2, r.15.1
- Sarbanes-Oxley Act — <http://www.soxlaw.com/>
- Software and Information Industry Association (SIIA) — q

## Conclusions

Disposal is the final chapter in the IT asset lifecycle, and it represents a mounting obstacle for IT professionals. According to the US Environmental Protection Agency (EPA), 134.5 million IT assets currently sit idle in America alone, and a scant 18 percent of these are likely to be recycled. On a global scale, the problem is only magnified. Tackling this problem requires that we answer the questions posed at the beginning of this document by applying rigorous disposal policies.

Regulatory compliance, fiduciary accountability, and environmental stewardship present an array of risks to IT professionals who must balance these considerations, whether they choose to refurbish, sell, donate, or dispose of technology assets. As illustrated here, organizations can abate these risks by making adequate investments in scoping and planning, analyzing impacts, soliciting input, and fostering consensus in the systematic development of comprehensive IT disposal policies. Employing such a policy will enable you to effectively address the ecological, regulatory, legal, and financial challenges you face each time you retire an asset.



## About the Authors



Howard Hastings is CA's ITAM Evangelist, Chairman of the Board at TagVault.org, and was recently named an IAITAM Fellow. He leverages a 30-year career in IT Service Management (ITSM)—as a practitioner, corporate manager, software executive, and entrepreneur—to influence product direction and expand market awareness of CA's ITAM solutions. Hastings joined CA when it acquired DecisionRight in 2007, where he was co-founder and VP of Solutions. In this role, he developed software recognition, augmented content for software inventory/asset management tool publishers, and delivered software license compliance services to IT organizations. At DecisionRight, Hastings also played a role in drafting early versions of the ISO 19770-2 ("Software Data Tag") and ISO 19770-3 ("Entitlement") standards. Prior to that, he held leadership positions with Remedy, Comdisco, and ReliaStar Financial. Hastings is a frequent speaker and author for trade publications and often serves as an expert witness in software copyright infringement and counterfeiting litigation. In 2007, he was recognized as a SAM Practitioner of the Year by the IBSMA. Hastings has also revised and taught the Certified Software Manager (CSM) and Advanced Software Manager (ASM) curriculums of the Software & Information Industry Association (SIIA) delivered by LicenseLogic.



Shawn Sande is a Senior Marketing Strategist in CA's Service Management Product Marketing organization. He is a seasoned industry veteran with over 15 years of professional marketing and business development experience, including 14 years in the information technology industry. In addition to two years in IT Asset Management product marketing at CA, Sande spent two years at Microsoft Corporation as a Senior Marketing Manager in Microsoft's Business Solutions business unit. Prior to that, he filled several key product marketing and marketing communications roles during a ten-year stint with mid-tier enterprise asset management vendor AssetWorks, Inc. Sande began his career in the management training program of Enterprise Leasing Company of Texas. He is Pragmatic Marketing® Certified in Product Marketing and a past member of the American Marketing Association (AMA) and the Society of Competitive Intelligence Professionals (SCIP).