

From Assets to Accountability:

The Property Manager's Guide to Secure IT Asset Disposition & Value Recovery

How property managers protect sensitive data, maintain asset accountability, and recover value from retired technology



Chapter One

The Property Manager's Mandate: Accountability, Security, and Value

A Different Kind of Property Responsibility

Property managers are responsible for knowing what an organization owns, where its assets are located, who has custody of them, and what happens when those assets are retired.

IT equipment adds another layer to that responsibility. Unlike most corporate property, retired technology may retain both financial value and sensitive data.

Laptops, desktops, servers, storage systems, mobile devices, networking equipment, and even multifunction printers can contain data-bearing devices. When these assets are transferred, sold, recycled, returned, or destroyed, the organization must account for both the equipment and the information it may contain.

That makes IT asset disposition an asset accountability, data security, and financial stewardship responsibility.

For property managers across large enterprises, government agencies, and government contractors, assets may be distributed across offices, warehouses, data centers, remote locations, and individual departments. Some may contain regulated, proprietary, government, customer, or employee information. Others may retain meaningful resale value.

Once equipment is removed from service, delays and unclear ownership create risk. Assets sit in storage, inventory records become outdated, data-bearing devices are overlooked, and equipment with resale potential loses value.

A mature disposition program addresses these issues together. The objective is to maintain control until the asset has been reconciled, its data securely resolved, its remaining value addressed, and its final disposition documented.

What's at Stake

Focus Area

Why It Matters



Security & Data Protection

Retired IT equipment may contain sensitive information. One overlooked data-bearing device can expose data after retirement.



Asset Accountability

Property records must remain connected to physical assets. Missing equipment and undocumented transfers create accountability gaps.



Financial Stewardship

Eligible IT equipment may retain recoverable value. Delays and poor handling can reduce Secure Value Recovery.



Documentation & Proof

Final disposition requires records showing what happened. Without documentation, you cannot prove the asset lifecycle was properly closed.

The Cost of Lost Control

Small process gaps can create larger problems:

- Assets cannot be located or reconciled.
- Data-bearing devices remain inside retired equipment.
- Chain of custody breaks during handoffs.
- Reusable equipment sits idle and loses value.

The result can be:

- Data exposure
- Audit or compliance issues
- Inventory discrepancies
- Lost value recovery opportunities

Property Manager Takeaway:

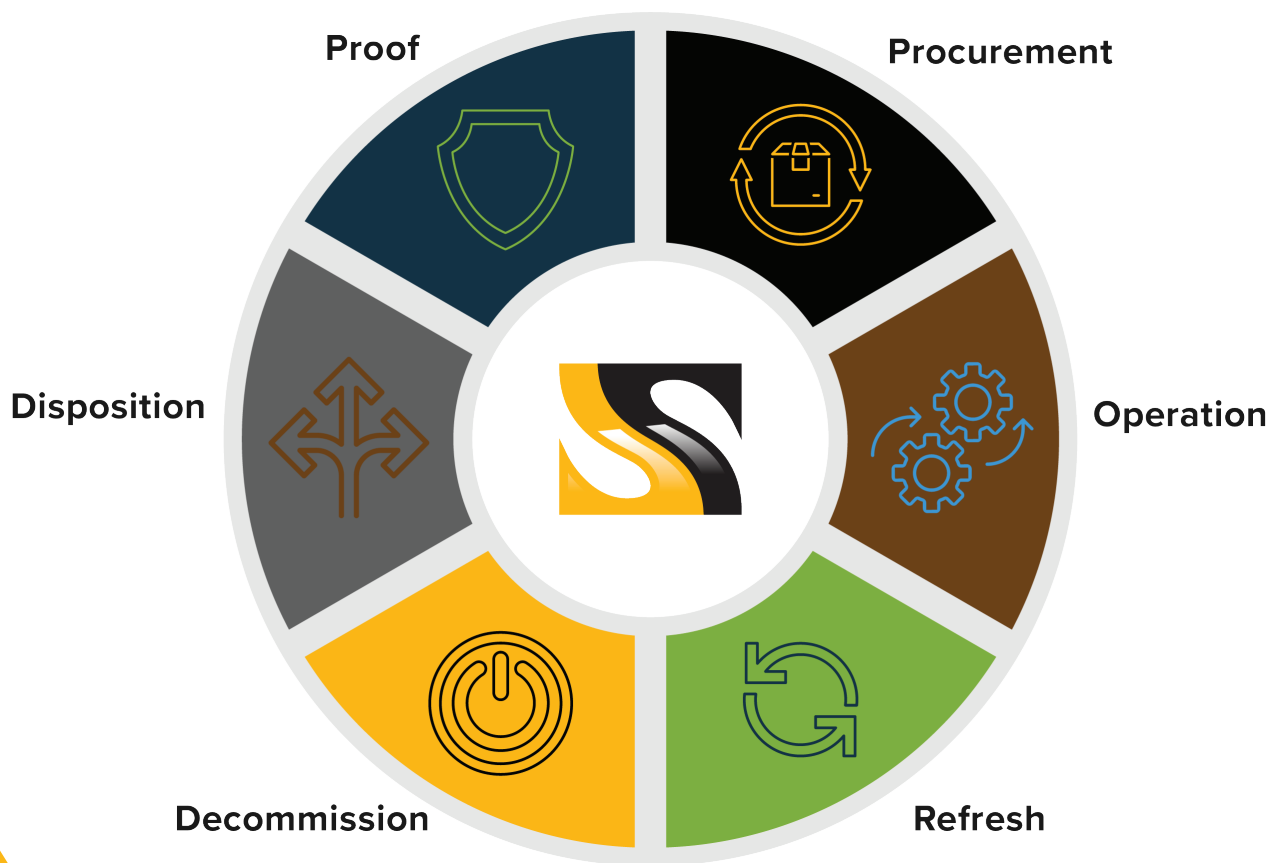
Strong asset stewardship maintains visibility from retirement through final disposition. If you cannot account for the asset, its data, and its final outcome, the lifecycle is not complete.

The Technology Lifecycle, Completed With Proof

Retiring an IT asset from the property inventory does not end the organization's responsibility for it. The asset still carries potential data risk, financial value, and accountability requirements through final disposition.

A complete lifecycle connects every stage, from procurement through disposition, with documented proof of the outcome.

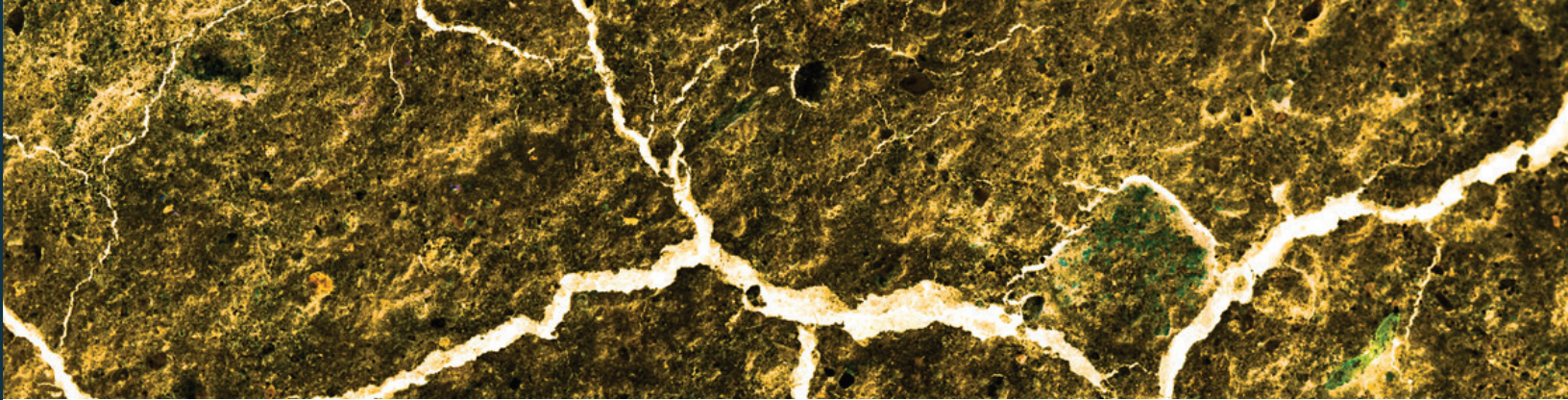
For Property Managers, the final step is knowing the asset is no longer just off the books. It is fully accounted for.



99%+
Accuracy

3-5
Business Day
Certificates of Destruction





Chapter Two

Where Assets, Data, and Value Slip Through the Cracks

When Asset Visibility Starts to Fade

Most disposition problems do not begin with a major failure. They begin when an asset moves outside the normal property management process.

A laptop is placed in a storage room after a refresh. Servers are removed from a rack but remain on an inventory list. Equipment moves from IT to Facilities without a documented handoff. A pallet waits for pickup while reusable technology continues to age.

At the same time, assumptions begin to replace verification.

Someone assumes the drives were removed. Someone assumes the inventory is accurate. Someone assumes the equipment has no resale value. Someone assumes another department is responsible for what happens next.

For Property Managers, this creates a unique challenge. Retired IT equipment is

still physical property, but its disposition involves responsibilities that may span IT, Information Security, Finance, Procurement, Facilities, and outside vendors.

Every handoff creates an opportunity for asset records and physical reality to move further apart.

The result may be an inventory discrepancy, an overlooked data-bearing device, an undocumented transfer, or an asset that loses recoverable value while waiting for a decision.

Strong IT asset disposition replaces those assumptions with a controlled process. Assets remain accounted for, data-bearing devices are identified, custody is documented, and equipment is moved efficiently toward secure reuse, remarketing, destruction, or recycling.

External Pressure Points

External Factor

Why It Matters



Distributed Assets

Multiple offices, warehouses, data centers, and remote locations make consistent asset accountability harder.



Departmental Handoffs

Transfers between IT, Property, Facilities, Finance, and vendors create opportunities for ownership and custody to become unclear.



Data-Bearing Devices

Drives and embedded storage can remain inside equipment even when assets are believed to be data-free.



Delayed Disposition

Idle equipment occupies space, complicates inventory, and can lose recoverable value while awaiting disposition.

Internal Breakdowns That Create Risk

Property Managers rarely control the entire IT asset lifecycle alone.

IT may decommission the equipment. Information Security establishes data requirements. Property Management maintains asset accountability. Finance has an interest in recovered value. Procurement manages vendor relationships. Facilities may provide staging or storage.

Each group has a legitimate role, but gaps appear when those responsibilities are not connected by one documented process.

Inventory records may no longer match the equipment in storage. Data-bearing devices may be missed during decommissioning. Assets may move between locations without documented custody. Equipment eligible for Secure Value Recovery may remain idle because no one owns the next step.

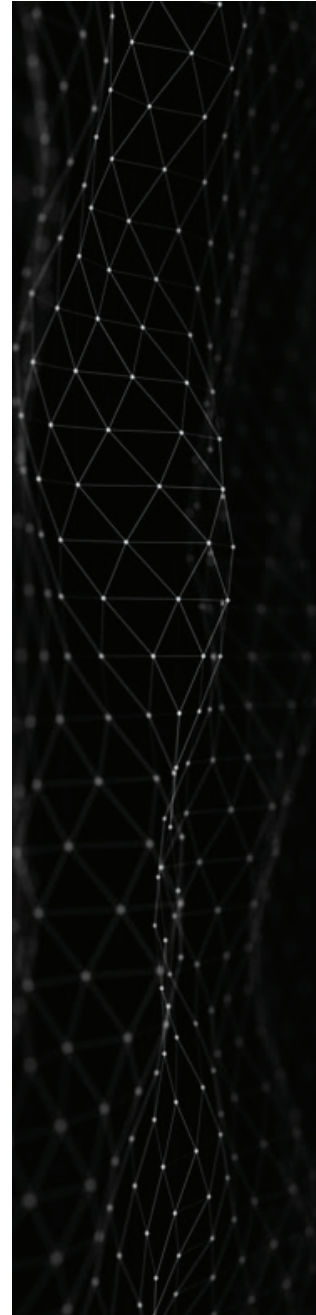
The problem is not the number of teams involved.

The problem is losing a single source of truth as the asset moves between them.

Property Manager Takeaway:

Clear ownership and documented handoffs keep physical assets, inventory records, and disposition outcomes aligned.

What Keeps the Property Manager Up at Night



Accountability does not end when an asset leaves service. Every gap in control creates uncertainty. Every missing record creates questions. Every undocumented asset becomes a security concern.



Where Control Slips Away

Most disposition failures happen in the space between retirement and resolution.

An asset may have been removed from service, but that does not mean its lifecycle is complete. Until the equipment is inventoried, its data requirements are resolved, its disposition path is determined, and the outcome is documented, the organization still has unfinished business.

Delays make that harder. Asset records become less reliable as equipment moves or sits in storage. Custody becomes harder to reconstruct. Equipment condition can deteriorate. Opportunities for Secure Value Recovery can diminish.

For Property Managers, the goal is to keep the physical asset and its record connected throughout this transition.

Philosophy Shift: From Disposal to Asset Stewardship

Traditional disposal asks a simple question:

How do we get rid of this equipment?

Asset stewardship asks better questions:

Where is it? What data does it contain? What should happen to it? What value may remain? Can we prove the final outcome?

That distinction changes IT asset disposition from a removal task into a controlled extension of property management.

Security and value recovery are not

competing objectives. A well-managed process determines which assets can be securely sanitized and remarketed, which require physical destruction, and how each outcome will be documented.

The objective is not simply to make retired equipment disappear.

It is to close the asset lifecycle with control.

Asset stewardship does not end when equipment leaves your facility. It ends when the outcome is documented.

Where Assets, Data, and Value Slip Through the Cracks



Risk increases when visibility decreases.

For Property Managers, the objective is to maintain accountability from the moment an IT asset leaves service until its data, value, and final disposition are resolved.





Chapter Three

Evaluating ITAD Partners Who Handle Your Assets and Data

When Your Assets Leave Your Control

Every disposition program reaches the same point: physical custody of your organization's assets moves to someone else.

Retired laptops, desktops, servers, storage systems, networking equipment, mobile devices, and other electronics must eventually be collected, transported, processed, remarketed, recycled, or destroyed.

That makes selecting an ITAD provider more than a purchasing decision.

The provider becomes part of your asset accountability process.

Property Managers need confidence that assets remain controlled after pickup,

data-bearing devices are identified and protected, inventory is accurately reconciled, and eligible equipment is evaluated for Secure Value Recovery.

The challenge is that these responsibilities do not disappear when the truck leaves your facility.

Your organization still needs to know what was collected, where it went, what happened to the data, which assets were remarketed or recycled, and whether the final records reconcile with the property transferred.

A strong ITAD partner preserves that visibility from pickup through final disposition.

Property Manager Takeaway:

Custody may transfer to an ITAD provider. Accountability for the outcome does not.

The Property Manager's Reality

Property Managers coordinate assets across teams, facilities, and locations. IT may decommission equipment, Security sets data requirements, and Finance tracks recovered value, but Property Management still needs to account for the final outcome.

A pickup receipt is not enough. You need records connecting transferred assets to what was received, processed, remarketed, recycled, or destroyed.

You also need protection against what may have been missed. Servers, printers, and other equipment can contain overlooked data-bearing devices.

At the same time, security should not eliminate value recovery. Assets that can be securely sanitized and reused should be evaluated for remarketing rather than automatically recycled.

You don't need a vendor that simply removes equipment. You need a partner that can account for what happens next.

What Asset Accountability Looks Like in Practice

Strong ITAD providers replace assumptions with documented controls.



Independent certification of secure data destruction policies, procedures, and operations.



Certified downstream controls and responsible reuse and recycling practices.



Sanitization methods aligned with recognized data-security guidance.



High-assurance physical destruction capabilities for HDDs and solid-state media when required.



Securis Triple Check Guarantee

Layered verification helps identify hidden or overlooked data-bearing devices during processing.



DriveSnap AI

Photographic documentation and AI-assisted serial-number capture help connect processed data-bearing devices to final records.

3-5 Business Day

Certificates of Destruction

Timely reconciliation and documentation help organizations close property records and reduce unresolved inventory.

120,000+

Positive Feedback Ratings

Long-standing reliability in secure value recovery, demonstrated at scale.

The value of these controls is simple: they replace assumptions with evidence. They strengthen chain of custody, improve inventory integrity, and provide the documentation needed to demonstrate accountability long after equipment leaves service.

Property Manager Takeaway:

Real accountability replaces assumptions with evidence and turns process into protection.

What Good Looks Like for Property Managers



The Standard Is Simple

A Property Manager should be able to answer three questions about every disposition project:

Where did the assets go?

What happened to the data?

What happened to the remaining value?

When your ITAD partner can provide documented answers to all three, disposition becomes a controlled extension of asset stewardship rather than an uncertain handoff.



Chapter Four

The Plan: A Clear Path From Retirement to Final Disposition

A strong IT asset disposition program keeps property accountability, data security, and value recovery connected from the moment equipment leaves service through final disposition.

This chapter provides a practical framework Property Managers can use to maintain control, reduce risk, and document the outcome of every retired IT asset.

A. Maintain Control From Retirement to Final Disposition

When IT equipment leaves service, it enters a transition period where ownership can become unclear and visibility can weaken. Defined processes keep assets controlled until their final disposition is documented.

1. Stage Assets Securely

Retired IT assets should remain in controlled storage until pickup. Organize equipment by disposition requirements and restrict access to prevent assets from being removed, mixed, or transferred without documentation.

For assets containing sensitive data, use additional controls appropriate to organizational policy and security requirements.

Property Manager Takeaway:

Secure staging keeps retired assets controlled and accounted for.



2. Determine the Right Disposition Path

Not every IT asset should receive the same treatment. Condition, data sensitivity, organizational policy, and reuse potential should determine what happens next.

- Sanitize and Reuse: Securely erase eligible equipment for redeployment or remarketing.
- Physically Destroy: Destroy data-bearing media when sanitization is not appropriate or policy requires destruction.
- Recycle: Responsibly process equipment that cannot be reused or remarketed.

Property Manager Takeaway:

The right disposition path protects data while preserving recoverable value where appropriate.

3. Decide on On-Site or Off-Site Processing

On-site destruction may be appropriate for sensitive assets or environments where transportation adds unnecessary risk. Off-site processing can support most enterprise disposition programs when assets remain protected by documented chain of custody, secure transportation, and verified processing.

A hybrid approach can address mixed asset populations with different security requirements.

4. Control Assets Before Pickup

Assets awaiting disposition should remain connected to property records. Confirm quantities, locations, asset identifiers, and custody before equipment leaves the facility.

Avoid allowing retired technology to accumulate indefinitely. Long storage periods increase inventory complexity, consume space, and can reduce Secure Value Recovery opportunities.

5. Control Day-0

Day-0 establishes the starting point for accountability. Before equipment leaves your facility, confirm what is being transferred and document the handoff. A clear baseline makes it easier to identify discrepancies and reconcile every asset at the end of the process.

Day-0 Checklist

- ☒ **Disposition authorized**
- ☒ **Assets inventoried and verified**
- ☒ **Data-bearing equipment identified**
- ☒ **Asset counts confirmed**
- ☒ **Chain of custody documented**
- ☒ **Vendor handoff recorded**

6. Reconcile Assets

Reconciliation proves that the assets transferred match what was received and processed.

Compare internal property records with the ITAD provider's inventory, investigate discrepancies, and document exceptions. Data-bearing devices discovered during processing should also be identified and connected to the final disposition record.

Accurate reconciliation provides Property Management with the evidence needed to close records confidently.

Property Manager Takeaway:

Reconciliation turns disposition into a verifiable property control.



B. Governance & Documentation

IT asset disposition should be integrated into property policies and recordkeeping rather than treated as a separate recycling activity.

Define who authorizes disposition, who establishes data requirements, who approves reuse or destruction, and what documentation is required to close the property record.

Clear ownership prevents assets from becoming stranded between Property Management, IT, Security, Finance, Procurement, and outside vendors.

C. Vendor Due Diligence

The ITAD provider becomes part of your asset accountability process. Due diligence should evaluate security controls, chain of custody, inventory procedures, data destruction capabilities, Secure Value Recovery processes, reporting, and downstream recycling practices.

On-Site Visit: Non-Negotiable

Before selecting an ITAD provider:

Inspect the facility

Review physical security, restricted areas, surveillance, access controls, and asset storage.

Follow the asset workflow

See how equipment is received, inventoried, staged, processed, and reconciled.

Observe data handling

Review how data-bearing devices are identified, sanitized, destroyed, and documented.

Evaluate Secure Value Recovery

Understand how eligible equipment is tested, securely sanitized, remarketed, and reported.

Review final documentation

See inventory reports, Certificates of Destruction, reconciliation records, and client reporting tools.

D. Build a Repeatable Process

Strong ITAD programs replace one-off disposal decisions with consistent controls for custody, security, reconciliation, documentation, and Secure Value Recovery.

A repeatable process keeps every asset accountable from retirement through final disposition, regardless of location, department, or project size.

E. Protect Value Without Compromising Security

Security and value recovery should support each other.

Eligible equipment can be securely sanitized and moved into reuse or remarketing channels, while assets requiring destruction follow the appropriate security path.

The key is making that determination deliberately rather than allowing every retired asset to default to recycling or destruction.

A mature ITAD program protects the data first, then preserves recoverable value wherever security requirements allow.





Chapter Five

The Decision Point: Turning Insight Into Action

A strong IT asset disposition program does not end with understanding the risks. It requires a defined process for what happens when equipment is ready to leave your organization.

You now know where accountability can break down, how data-bearing devices create additional risk, and why recoverable value should be considered before equipment is destroyed or recycled.

The next step is applying those principles to your own asset environment.

Every Strong Disposition Program Starts Here

A consultation begins by understanding what you have, where it is located, and what needs to happen to it.

Your team reviews asset types and quantities, locations, staging and storage practices, security requirements, chain of

custody, inventory expectations, reporting needs, and opportunities for Secure Value Recovery.

From there, the appropriate disposition path can be established for each asset category.

Define Your Security Requirements

Not every asset requires the same treatment.

The consultation identifies which equipment can be securely sanitized for reuse or remarketing and which data-bearing devices require physical destruction. Requirements for on-site processing, witnessed destruction, secure transportation, or additional documentation can also be established before assets move.

Defining these requirements early prevents uncertainty later and ensures security decisions support both organizational policy and property accountability.

Identify Secure Value Recovery Opportunities

Security comes first, but secure disposition does not mean every asset should be destroyed.

Eligible laptops, desktops, servers, networking equipment, and other technology can be evaluated for reuse or remarketing after applicable data requirements are satisfied.

The consultation helps determine which assets may qualify for Secure Value Recovery and how those assets can move efficiently toward the appropriate resale channels.

Property Manager Takeaway:

Define the security requirements before the assets move.

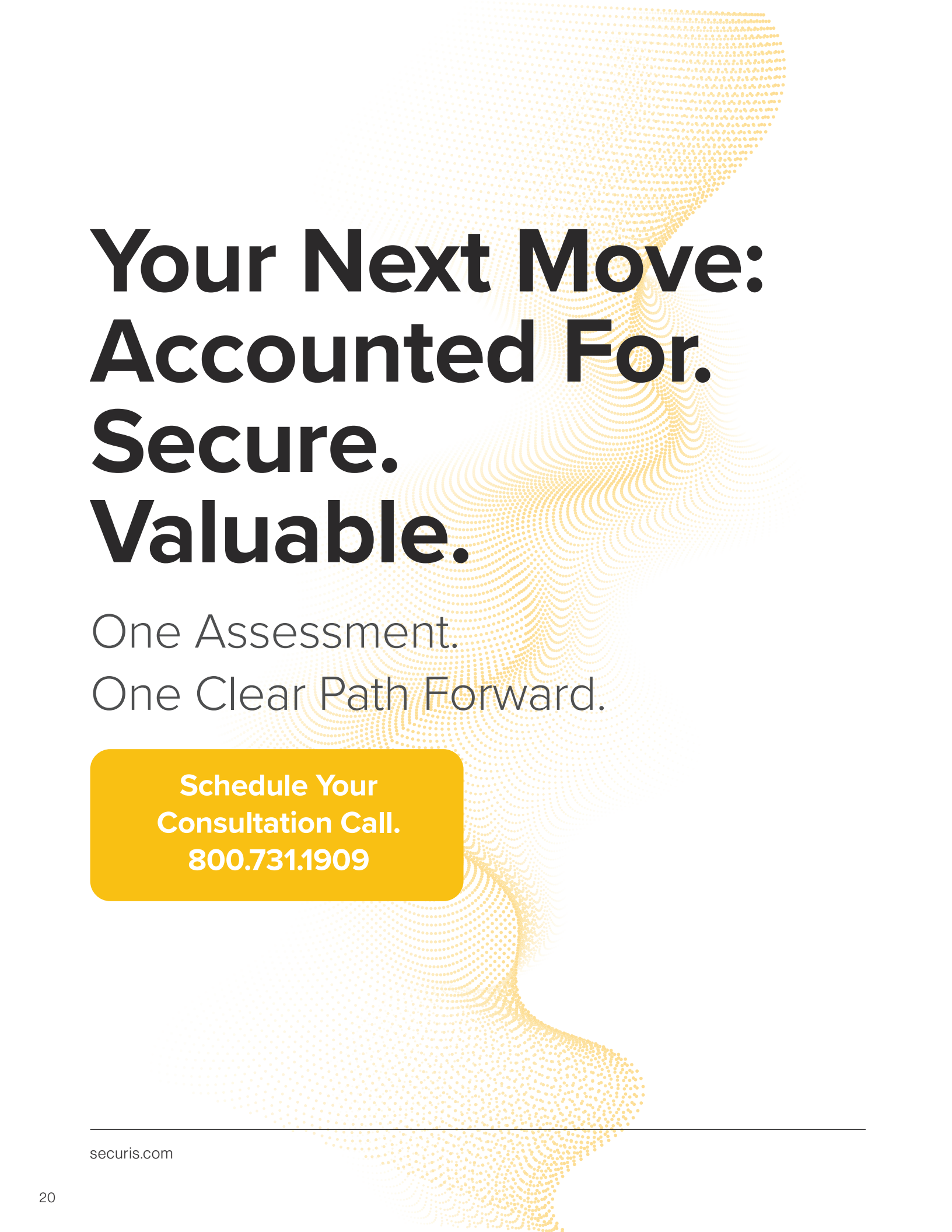
Schedule Your IT Asset Disposition Assessment

In one discussion, gain a clearer understanding of your asset inventory, security requirements, disposition options, Secure Value Recovery opportunities, chain-of-custody needs, and documentation requirements.

Turn retired IT equipment into a controlled, documented disposition process from pickup through final resolution.

Property Manager Takeaway:

Protect the data first, then preserve recoverable value where appropriate.



Your Next Move: Accounted For. Secure. Valuable.

One Assessment.
One Clear Path Forward.

**Schedule Your
Consultation Call.
800.731.1909**



Chapter Six

When Asset Disposition Goes Right and Wrong

Strong IT asset disposition is usually invisible. Assets are accounted for, data is protected, value is recovered where appropriate, and documentation closes the property record.

When the process fails, the consequences are much easier to see.

The following examples show why Property Managers need visibility beyond the moment equipment leaves their facility. What happens next can determine whether an asset becomes a successful disposition, a lost opportunity, or a serious data-security problem.

Success Story 1: The 86 Drives Nobody Knew Existed

Securis was hired to perform on-site shredding for a financial services company disposing of eight server cabinets. The client reported that all storage devices had already been removed.

They had not.

Through its Triple Check process, Securis identified 86 drives still installed, including 72 SSDs and 14 HDDs. Each represented sensitive data that could have remained inside equipment believed to be data-free.

Securis removed, documented, and securely destroyed every drive on-site. DriveSnap AI provided photographic documentation and serial-number capture, with Certificates of Destruction documenting the outcome.



Success Story 2: Leading Payment Processor – When the Parts Were Worth More Than the Whole

A leading payment processor engaged Securis to decommission its on-premises data centers in Delaware and New York, including a significant number of enterprise servers.

Using AI-powered market intelligence and its global buyer network, Securis determined that parting out the servers could generate greater returns than selling them intact. HDDs and SSDs were securely wiped using Blancco Drive Eraser, preserving eligible components for resale without compromising data security.

The strategy generated \$132,630 in additional revenue, a 54% increase over prevailing market rates for selling the servers intact. The result demonstrates how a security-first ITAD strategy can uncover greater value without compromising data protection.



Failure Example 1: Morgan Stanley

Morgan Stanley learned that transferring equipment to a vendor does not transfer accountability for the outcome.

Deficiencies involving the sanitization and disposition of retired hardware resulted in devices containing customer data remaining at risk. In 2020, the Office of the Comptroller of the Currency imposed a \$60 million civil penalty related to deficiencies in the bank's oversight of the decommissioning process and third-party vendor.

The lesson for Property Managers is straightforward: selecting a vendor is only part of the responsibility. Organizations also need documented chain of custody, defined processing requirements, reconciliation, and proof of final disposition.

Control That Prevents It: Vendor due diligence, documented chain of custody, inventory reconciliation, verified data sanitization or destruction, and final disposition records.

Sources: Office of the Comptroller of the Currency (OCC), 2020; U.S. Securities and Exchange Commission (SEC), 2022



Failure Example 2: Affinity Health Plan – The Hard Drives Hidden in Plain Sight

Affinity Health Plan returned leased digital photocopiers without removing or sanitizing the hard drives inside them.

The problem became public when a copier purchased during a CBS News investigation was found to contain sensitive patient information, including medical records and Social Security numbers.

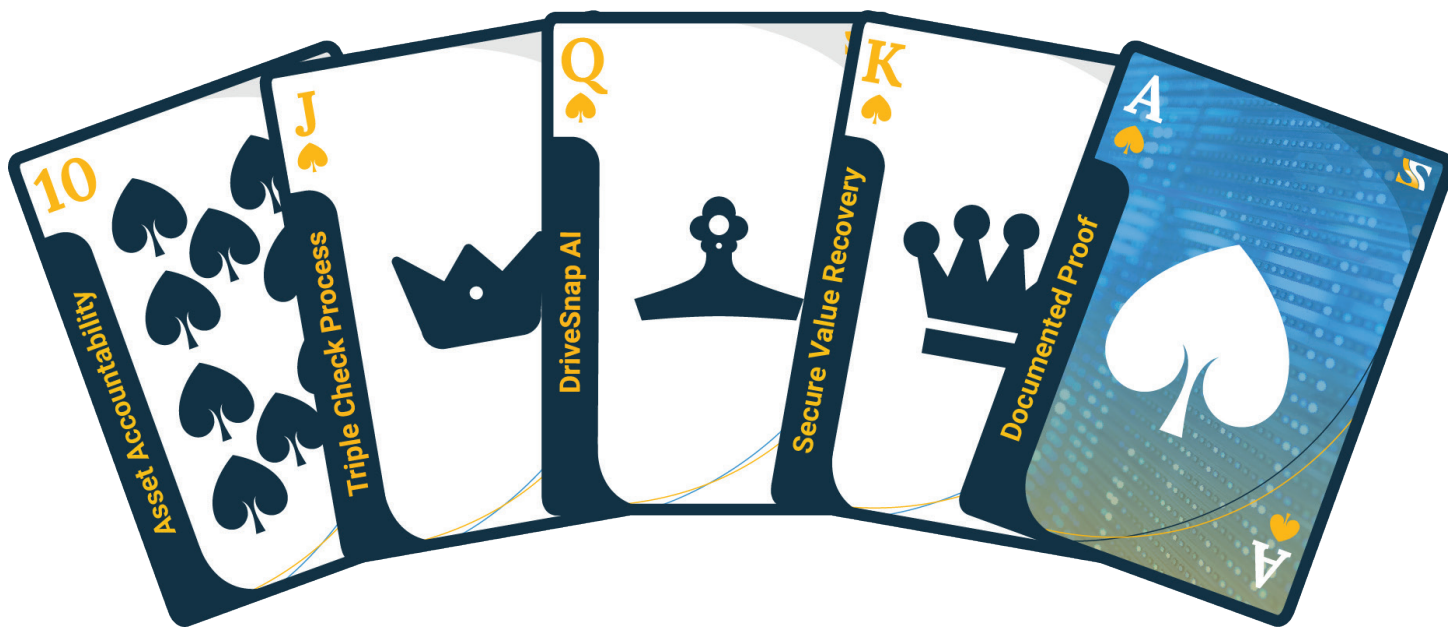
More than 344,000 individuals were affected, and Affinity ultimately reached a \$1.2 million HIPAA settlement with the U.S. Department of Health and Human Services.

The failure was deceptively simple: the organization disposed of the physical property without fully accounting for the data-bearing devices embedded inside it.

Control That Prevents It: Physical inspection, identification of embedded storage, inventory reconciliation, appropriate sanitization or destruction, and documented proof of disposition.

Source: U.S. Department of Health and Human Services (HHS)
HIPAA Enforcement Action, Affinity Health Plan

The Asset Stewardship Royal Flush



Hold the winning hand in accountability, security, and value recovery.



Make the Winning Move

Protect the Asset. Secure the Data. Preserve the Value.

Retiring IT equipment is more than removing property from an inventory.

Every asset needs a documented outcome. Know where it went, what happened to the data, and whether its remaining value was protected.

Strong Property Managers maintain accountability through the entire disposition process, from retirement and custody transfer through Secure Value Recovery, recycling, or destruction.

Close the asset lifecycle with confidence.
Call Securis. (800) 731-1909 | [Securis.com](https://www.securis.com)

NORTHERN VIRGINIA HEADQUARTERS
3900 STONECROFT BLVD. SUITE F, CHANTILLY, VA 20151
(800) 731-1909 | info@securis.com