



IT Asset Disposal Program Management Guide

Table of Contents

Background Information	2
Section 1: IT Asset Disposition Program Overview	4
Section 2: Financial Planning & Performance	7
Section 3: Requirements for Contracting Service Providers	10
Section 4: Sourcing & Ongoing Due Diligence	13
Section 5: Physical, Logical & Administrative Security	15
Section 6: Ensuring Compliance	17
Section 7: Tracking Assets & Disposal Events	19
Section 8: Coordinating On-Site Activities	22
Section 9: Finalizing ITAD Projects & Report Management	24

Background Information

The following program manual is intended as a guide for any professional tasked with managing the disposal of surplus or unwanted computer and IT equipment. By adopting the techniques provided in this document IT managers and alike will be able to accomplish IT disposal management in a responsible, secure, compliant, cost conscious and efficient manner.

This document can be used as a source to inform your current program or can be converted into your new disposal policy. As further discussed in this manual, documentation of your ITAD policies and procedures are key to achieving various regulatory requirements, as well as a best practice for any business practice.

Although there is unlikely to be a one size fits all approach to creating an IT asset disposition program, it is the goal of this document to empower practitioners to establish systems built on a foundation of security, compliance and business management best practices. We hope that even the most seasoned professional will be able to walk away from this tutorial with at least a few improvements to put into action.

The exact details of an IT Asset Disposition program will depend on each company’s unique initiatives and goals. However, there are some key financial, asset management, environmental, security, and regulatory compliance fundamentals that companies of all types should consider when performing IT equipment disposition or building an ongoing IT asset disposal program.

The remainder of this training document will be written from the perspective of a company that is drafting policies for the ongoing management of IT asset and retired electronic media disposition. It is written from this perspective to make the document as easy as possible to adapt or convert into your company’s policies.

Throughout the document there are abundant opportunities to select certain tools, methods, approaches and insert your company’s specific requirements or additional policies.

It should be noted that a policy like this document is a first step in program development and does not take the place of procedures and documented training of staff.

This manual was developed by the leadership team at IT Asset Management Group (ITAMG). ITMAG is an IT asset disposal and data destruction service provider with over 20 years of experience managing complex IT disposition projects and programs.

Frank Milia, NAID Certified Secure Destruction Specialist and Partner at ITAMG is the lead developer of the training guide. A special thanks is given to Charles Veprek, Director at ITAMG who provided significant support to the contents of this training guide and to Ramanpreet Kaur, Client Relationship Manager at ITAMG, for providing editing and content support.


For information and disposal program support please reach out to Frank Milia, CSDS.

Frank Milia


Partner


IT Asset Management Group

NAID Certified Secure Destruction
Specialist

 [516 284 8577](tel:5162848577) | [347 724 6018](tel:3477246018)

 frank@itamg.com

 itamg.com

 110 Bi County Blvd. Suite 106, Farmingdale NY,
11735

Section 1: IT Asset Disposition Program Overview

This document was last updated: XX-XX-XXXX

(The program should be reviewed at minimum once a year and updated as needed).

The purpose of this document is to establish and document the policies and methodology behind the policies of SAMPLE-COMPANY's IT asset and electronic data disposition program.

This program is built with the goal to ensure our organization disposes of surplus electronic assets and IT equipment of all types in an environmentally and socially responsible manner.

The following program policies also establish the framework for procedures to protect personally identifiable information (PII), protected health information (PHI), intellectual property (IP) or otherwise regulated, protected, and/or sensitive data during disposition and around the time of retirement.

These policies are also designed to ensure that our financial, operational, and business interests are met.

Overview of Program Goals:

1. Establish financial requirements and policies
2. Set vendor agreement and contract requirements
3. Name the program's responsible parties and chain of command
4. Name the program's stakeholders and interested parties
5. Provide overview of data destruction and security requirements
6. Establish environmentally responsible recycling practices
7. Ensure data protection and privacy regulatory requirements are met
8. Support operational efficiency
9. Set standards for asset management and event tracking

This program is informed by the best practices developed by the National Association for Information Destruction for data disposition, NIST 800-88 Guidelines for Media Sanitization and the Sustainable Electronics Recycling International's (SERI) Responsible Recycling (R2) standards. This program does not claim, or imply, to be certified by the aforementioned programs.

Named Responsible Parties:

It is necessary to name the responsible and trained parties that are actively engaged in asset and data disposition. This is an industry best practice, helps ensure better performance of a

program, and significantly reduces our organization’s breach and data protection regulatory liabilities.

The following Responsible Parties have direct responsibilities in the performance of this program. The parties responsible for coordinating with auditors, certifying bodies, or investigators should be noted below as well.

- Jane Doe – IT Director (*example, title or assignments may differ*)
Sample Description: Our IT director is responsible for all of this program’s policies, procedures and training of this program to all other responsible parties. The IT director will provide regular review of the program’s financial, security, operational and compliance performance. The IT director is responsible for vendor selection and due diligence. The IT Director will also act as the compliance officer and will be responsible for reporting to any auditors, regulators, or investigators in the case of a certification or breach.
- John Doe – IT Manager(s) (*example, title or assignments may differ*)
Sample Description: Our IT Manager is responsible for the day to day performance of the disposal activities documented in this program. This includes asset tracking, data destruction performance, scheduling and overseeing vendor services, collecting, and backing up project reports. The IT manager is responsible for ensuring his/her activities follow SAMPLE-COMPANY’s data security and regulatory compliance requirements.
- Jane Doe II – CIO (*example, title or assignments may differ*)
Sample Description: The CIO is responsible for approving and signing Master Service Agreements with vendor(s) that perform IT asset disposal and data destruction services. The CIO is also responsible for approving the budget for the IT disposal and data disposition services.

Named Stakeholders:

The following stakeholders have interest or general oversight in the performance of this program.

- Jane Doe II – CIO (*example, title or assignments may differ*)
Sample Description: Our CIO is responsible for the overall performance of the IT budget and technology operations.
- John Doe II – CFO (*example, title or assignments may differ*)
Sample Description: Our CFO is responsible for the overall financial performance of vendors and that companywide purchasing procedures are followed.

- John Doe III – CISO (*example, title or assignments may differ*)
Sample Description: Our CISO is responsible for the security of our information systems and protecting confidential data from unauthorized access.
- Jane Doe III – VP, Facilities Management (*example, title or assignments may differ*)
Sample Description: Our VP, Facilities Management is responsible for the associated building operations, physical security, real estate, and logistics planning.
- John Doe IV – IT Asset Manager (*example, title or assignments may differ*)
Sample Description: Our IT Asset Manager is responsible for tracking IT assets and removing retired and disposed of assets from our asset management program.

All responsible parties and named stakeholders are to be trained and aware of the contents of this document and program, including notification of when the program is revised in anyway.

Named Interested Parties:

An interested party is any party, person or group outside of the company that may be affected by the various aspects of the IT asset disposition program. The following interested parties are named.

Examples are provided below. Actual named interested parties and descriptions may differ in your program.

- Customers

Sample Description: It is in our organization's best interest to protect our customer's sensitive and proprietary information. Any case of a data breach or an environmental non-conformity related to improper disposal of IT assets and media could harm our brand and customer confidence.

- Auditors & Regulators

Sample Description: Any applicable certifying bodies, regulatory agencies, environmental certifications, or IT auditors should be explicitly named here as an interested party. It is important to have established and well documented IT disposal and data protection policies, procedures, training, and performances to satisfy these interested parties.

- Our building management and neighbors

Sample Description: It is important that we are good neighbors and do not disturb or otherwise negatively impact our building. This includes but is not limited to making sure our

waste does not inappropriately inhabit hallways and that at time of disposal we follow the building requirements for the disposal activity, use of elevators, docks, loading zones or otherwise.

- Associated Vendors

Sample Description: It is important that we collaborate with our service providers to effectively meet the standards of our disposal program. We should take special care to update our vendor(s) when any changes to our process, needs, requirements, or significant business changes occur that will affect the vendor's ability to serve our organization appropriately.

- The environment and the world community

Sample Description: We take recycling hazardous electronics waste seriously and want to ensure our impact on the environment is as little as possible. Steps to ensure our environmental stewardship include but are not limited to reusing or selling electronic equipment for reuse whenever possible and contracting downstream vendors that can guarantee and prove responsible e-waste recycling practices.

Section 2: Financial Planning & Performance

Our organization must budget for IT disposal and data disposition and appropriate funds for proper e-waste recycling and data destruction services. Having the correct budget for asset and data disposition puts our organization at a decreased risk of a regulatory non-compliance or data breach event by ensuring we are in a position to contract qualified vendor(s) that can meet our requirements and can pass our due diligence process.

While it is important that we select vendor(s) that are able to provide competitive pricing on disposition services, choosing a custodian of our organization's PII or other sensitive data based solely on price is a poor practice that could lead to hiring unqualified vendors that do not meet the requirements of our disposition program.

The following financial and business planning policies will help our organization remain secure and compliant while ensuring our organization's financial interests are met.

Financial Planning

Each year we will define a budget for the spending on IT disposal and data destruction services as well as any potential value recoveries from the liquidation of our surplus computer and IT equipment.

We will need to coordinate with our vendor(s) or prospective vendor(s) to achieve financial planning. The following information will be needed to provide to vendor(s) and collaborate on any pricing exercise.

For Cost Forecasting:

- Collect historical disposal data for previous year(s). If asset level details such as model and specs are not available collect quantities of equipment by product type (Laptops, PCs, Printers, Servers etc.).
- Collect list of locations and what volume was generated by each location. If this information is not available at this time, provide an estimated quantity of devices managed at each location by product category.
- Note the details and account for any special projects, office closures, office relocations, data center moves, refresh projects or any other events that could result in a higher quantity of disposal events or volume from previous year(s).
- Note any significant changes in service level requirements for previous years. For example: Did our policies and procedures change? Did our logistics or tracking requirements change? Did our methods of destruction change?
- Account for any growth or downsizing that may have led to a smaller or larger infrastructure than past year(s).

For Value Return Forecasting:

In order to estimate what value returns will be recovered for a given period of time we will need to provide our vendor(s) with a list of equipment models and/or specs of equipment in order to find the current fair market value.

Using this information and whatever other reasonable information the vendor(s) requires to provide fair market values, we can work with the vendor to project the yearly returns based on what percentage of stock we believe we will be upgrading or otherwise disposing of this year.

This projection will be used as an estimate and goal only and will not affect the budget we put in place for accounting for the yearly costs of activity.

Ad hoc Project Pricing:

From time to time it will be in our organizations best interest to price specific projects such as data center decommissions, equipment refreshes or otherwise.

Again, we will need to provide our vendor(s) with as much detail as possible of the assets being disposed of, the services needed, and the logistics requirements for such projects including but not limited to the following.

- Asset attribute details, model, OEM part numbers, and specs such as RAM, processor and storage type and capacity.
- Logistics requirements including location(s), site requirements, packaging and moving needs, and any other services the vendor will need to provide on-site at our location(s).
- Condition of equipment or best estimate of the condition of the equipment
- Set an accurate timeline for release of equipment to vendor and deadline for services
- Confirm all service level requirements are accurate and conforms with our regular policies and procedures
- Only price projects with approved vendors or vendors that have been “pre-approved” by the responsible party to meet our program’s requirements

Improving Financial Results

The following administrative methods and operational steps can be taken to improve the IT asset disposal program’s financial performance.

Administrative:

- Perform regular audit of vendor quotations and corresponding invoices
- Regular audit of disposal reports and financial reconciliations of asset recovery payments or credits from vendor
- Regularly review asset management data and approve disposal of retired equipment in a timely manner to reduce value depreciation
- Address any irregular or poor financial performances with vendor(s) in a timely manner
- Retain back-up and parts machines only as reasonably needed and approve disposal of any over-stock equipment to reduce value depreciation
- Regular communication with vendor(s) to review costs, potential savings, and opportunities to recover more value on equipment being disposed of

Technical and Operational:

- Ensure our staff is performing all responsibilities required to ensure the physical security and good condition of our retired and over stock equipment. Lost, stolen or broken equipment will negatively impact our financial, data security, and environmental performance significantly.

- Ensure our asset management systems are accurate and up to date
- Make sure all requirements for selling equipment on secondary markets is performed including but not limited to removing any administrative passwords, BIOS password locks, Apple ID / iCloud, theft tracking software or similar have been removed or otherwise set to a factory default that can be provided to the vendor(s). Take all other necessary steps to remove “de-enroll” assets from our asset management, device management, or second party registries as applicable. Locked or enrolled equipment may not be sold by vendor(s) and in turn we will receive no credit back on equipment in this state.

Section 3: Requirements for Contracting Service Providers

Any vendor that acts as a custodian of our protected data or otherwise performs data disposition or IT asset disposal services for our organization must be formally contracted to do so. The ideal method for such contracting is by signing a Master Service Agreement (MSA) that covers the vendor(s)'s core responsibilities, financial obligations, regulatory compliance requirements, data security requirements, data privacy requirements, reporting requirements and environmental practices and assurances.

The MSA should be reviewed yearly to make sure all service levels are accurate and cover our program needs. The MSA should be renewed and kept current with all vendor(s).

Our organization must also perform and document due diligence of any data disposition provider to meet data protection regulatory requirements and our internal data security mandates.

Contract Requirements

The following are the minimum contract requirements our organization has for contracting any downstream recycling or data disposition providers.

Insurance:

Insurance requirements should be determined by your legal or compliance team and done so in the best interest of protecting the size and scope of your business. The below is an example of common insurance requirements for enterprise customers.

- The vendor must be contracted and provide proof of the following minimum insurance requirements

Commercial General Liability Insurance on an Occurrence basis:

Bodily Injury and Property Damage

Personal and Advertising Injury as defined by policy to include libel & slander

Broad form property damage liability.

Blanket Contractual Liability.

The minimum limit for Commercial General Liability insurance coverage shall be:

- Each Occurrence: \$1,000,000
- Annual Aggregate: \$3,000,000
- Products & Completed Operations Aggregate: \$1,000,000

Excess Liability limits of not less than:

- Each Occurrence: \$5,000,000
- Coverage to follow form of underlying policies.

Auto Liability Insurance for owned, leased, or hired vehicles, if any:

- 1,000,000 per Occurrence combined single limit bodily injury and property damage.

Professional Liability:

- \$1,000,000 per Claim/\$3,000,000 annual aggregate.

Network Security/Cyber/Privacy Breach Insurance is required if Vendor has access to Customer's data (including, but not limited to, information protected under HIPAA):

- \$3,000,000 per occurrence/\$3,000,000 annual aggregate.

Worker's Compensation Insurance: Statutory limits

Employer's Liability Insurance

- Bodily Injury by Accident: \$1,000,000 each accident
- Bodily Injury by Disease: \$1,000,000 each employee
- Bodily Injury by Disease: \$1,000,000 policy limit

Protecting Confidential Information:

The contracting agent is to ensure data privacy and confidential information policies and protections are reflected in the disposal vendor MSA and/or otherwise in an additional non-disclosure and confidential information protection agreement. Such agreement should include the vendor's agreement to be financially responsible for damages that result in negligence or other non-compliance with a regulatory data protection requirement or damage associated to a leak of intellectual property, PII or sensitive business information.

Indemnification:

The vendor shall be required to indemnify, defend and hold harmless our organization and affiliates, respective partners, officers, directors, employees, representatives, agents and assignees (each an "Indemnity") from and against any and all claims asserted against, imposed upon or incurred by an Indemnity due to, arising out of or relating to (i) any breach by vendor

of any representation or warranty under the Agreement; (ii) any death of or injury to any individual or loss of or damage to personal or real property of an Indemnity resulting from the negligent or illegal act or omission or the willful misconduct of the vendor.

It should be noted that our organization cannot be indemnified for our legal obligations to protect regulated confidential data. However, by appropriately contracting a vendor we can assign financial obligations to our vendor(s) in the event of a breach or non-compliance. In doing so we reduce our financial risk associated with a data breach resulting from data disposition activities.

Data Security:

An agreement must include data security requirements for the data disposition vendor including a commitment from vendor to exercise a degree of care consistent with the highest industry standards including but not limited to the following

- Vendor breach notification
- Breach response and corrective actions
- Data destruction procedures, practices, and documentation will be in accordance with the NIST 800-88 Guidelines for Media Sanitization

Environmental Requirements and Obligations:

The vendor must commit to recycling practices in accordance with one or more of the major third-party certifications (SERI R2 or e-Stewards). The vendor must commit to remaining certified to one of these standards for the length of the agreement.

Reporting Requirements:

The vendor must commit to our reporting standards including our minimum requirements to report device make, model, serial number, date of shipment, asset tag, location of shipment, weight, and data destruction services performed. Reporting should be made digitally available via email and web portal.

Vendor must guarantee backup data for at least one year from the reporting delivered to our organization and take reasonable measures to backup reporting data indefinitely.

Process & Billing Requirements:

Agreements must meet our organization's standard billing requirements. Insert those terms here or refer to AP/AR policy document(s).

Asset Recovery Terms:

The standard asset recovery terms should include the percentage revenue share back to our organization, and any other terms for the shipment of valuable equipment where there has not been an agreed upon pricing schedule before the time of shipment.

Vendor to agree to a reasonable process for vendor to provide ad hoc pricing for the liquidation of assets as needed by our organization.

Section 4: Sourcing & Ongoing Due Diligence

Our organization can be held legally responsible for a data protection non-compliance resulting from inadequate vetting of service providers. Our responsible party is tasked with performing vendor due diligence at time of sourcing and ongoing to mitigate these associated risks.

Due diligence when selecting a vendor and developing a compliant process extends further than executing a strong agreement with a vendor or relying solely on the vendor's credentials via third-party certifications.

The following due diligence activity must be satisfied for any vendor performing IT asset and data disposition services for our organization.

Document Third Party Certifications:

We must check directly with the third-party certifying body to confirm the current or prospective disposal vendor is certified and in good standing. This can be done directly on the R2, NAID, and/or e-Steward websites. In addition, digital copies of the vendor's certifications should be reviewed and saved for compliance purposes.

It is also important that the third-party certification is vetted, and this vetting is documented. This can be done by contacting the third-party certifying body and obtaining information on the standards and requirements of the respective certification and evaluating the merit of the vendor's third-party certification.

This should be done as a best practice and to display due diligence for data protection regulatory compliance.

Document Vendor Management Systems:

The vendor will be required to provide documents to display core competencies in environmental management, health & human safety, and data security. The policies and procedures should display adequate core competencies to meet the requirements of our stakeholders and program.

These documents should be active and integral policy and procedures from the vendor's management system to include the following:

- Mission and policy statement
- Breach and data security incident policies and procedures
- Employee NDA and Data Protection Acknowledgement Agreements
- Material management plan
- Security and data destruction policies and procedures
- Corrective & preventative action policies and procedures
- Visitor procedures
- Facility standards
- Transportation policies and procedures
- Hiring and screening policies and procedures
- Competence, awareness and training policies and procedures
- Customer satisfaction and complaint policies and procedures
- Vendor's downstream charts that document final destination of all applicable materials

The vendor is required to supply updates to these documents no less than once a year. Our organization is required to maintain such documents in case of an audit or regulatory non-compliance.

This should be done as a best practice and to display due diligence for data protection regulatory compliance.

Site Visit & Vendor Audit:

It is in our organization's best interest to investigate and document firsthand the capabilities and infrastructure of any vendor handling electronic waste or data destruction projects regardless of the reputation, certifications, or track record the vendor may present.

A documented site visit is a powerful display of performing due diligence and to mitigate liability of an unlikely breach or exposure that could occur from an improper computer disposal.

Visiting a vendor or taking a virtual tour of the vendor's facility is required due diligence.

During a site visit the following items should be investigated:

- Physical security and access controls of vendor's facility
- Process for tracking shipments in and out of facility
- Process, tools, and infrastructure for performing data destruction including shredding machinery, software, and hardware infrastructure for data erasure

- Inventory management tools and asset tracking process for assets at vendor's facility
- Inspection of health and human safety practices and conditions
- Vendor's competencies in dismantling, refurbishing, technical support, information security, and packaging capabilities
- Investigate the vendor's capability to meet our organization's volume of assets

The results of a site audit should display adequate core competencies to meet the requirements of our stakeholders and program.

Once we have performed and documented a site audit, a reoccurring schedule to review any major process or facility changes should be scheduled for no less than once a year.

References:

When onboarding a new vendor at least two other commercial references should be supplied by the vendor. The vendor references should be interviewed, and the results of the interview be documented.

Vendor references should meet the following:

- Similar equipment volume and financial scale to our organization's program
- Have a service engagement of over a year with prospective vendor
- Have a similar service engagement to the services our organization requires

Section 5: Physical, Logical & Administrative Security

It is our organization's legal responsibility to protect against unauthorized access to protected data up and to the point of reasonable data destruction at our site of transfer to a contracted service provider.

The following are the minimum physical and logical security steps that must be taken in relation to this data disposition program.

Physical Security Practices:

Retired equipment is at particular risk of theft, loss, or other unauthorized access. The responsible party must ensure physical access to surplus is limited to only parties that are trained in data protection and data disposition practices and otherwise have legitimate work requirements to access such space.

Retired equipment and media should meet the following requirements:

- Be stored in a locked location where key access or scan-in / scan-out logs are managed and recorded
- We require a detailed inventory of any equipment being stored for disposal to be taken at time of putting equipment into storage and this inventory to be monitored and confirmed at time of approval to dispose and disposition. Any changes to the stored equipment should be updated in the inventory including but not limited to redeployment, additions, subtractions, or when final disposition occurs.
- Loose non-paper media (ex. optical disks, tapes), SSDs (ex. flash drives, smartphones), and HDDs, to be contained in tamper proof bins, boxes, or containers (supplied by data disposition vendor if applicable)
- Equipment to be stored in a professionally alarmed location with security camera coverage. Video recordings should be saved for at least 90 days. Access to video footage must be reasonably searchable to pull video recordings by date, time, and location.

It should be noted that locked totes, containers, or sealed boxes are not inherently a security measure, and instead are a deterrent, a means of displaying to potential accessors that restrictions exist, and as a method for identifying that tampering may have taken place. It is important that we do not rely on these types of containers as a security measure and make sure these containers are stored in a secure and monitored location.

Furthermore, a vendor that supplies us with media containers in no way takes responsibility for the security of the media until it is transferred to the vendor and removed from our site. Again, this is important for the responsible parties to be aware of and take all necessary measures to protect the access to retired media until destruction and/or disposal has taken place.

Logical Security Practices:

Retired media is at a threat to exposure during storage at our site, transfer, or shipping, and if disposed of to a poor performing contractor.

It is because of this our organization requires the following logical security practices:

- Erasure data destruction to the NIST 800-88 standard is performed on all non-encrypted media prior to shipping, transfer, disposal, or reuse inside the organization.
- Where erasure of the non-encrypted media is not possible or effective, a physical method of destruction must be performed such as shredding, pulverization, or degaussing of the media (please note degaussing is only effective for magnetic media and should not be used for destruction of flash or SSD media).
- Encrypted media may be relocated, shipped, or otherwise securely transported for reuse within the organization or to a contracted vendor for disposal and destruction
- Media and data containing devices may be categorized and classified according to risk of exposure to our organization. In the case of “top secret” classifications our

organization will require data destruction, including for encrypted media, to be performed prior to any transfer or disposal to a data disposition provider.

- Our organization recognizes and approves all tools and methods in the NIST 800-88 Guidelines for Media Sanitization to be deployed on an as need basis.

Our organization's security stakeholder should provide content here on the specific media classifications, data security levels, policies and requirements for tools, and methods for encryption and data destruction. If a data disposition security document already exists please reference to this document in this section.

Administrative Security Practices:

Our organization understands that a disciplined administrative approach to data security is required for our data disposition program to be effective.

The responsible party is tasked with making sure the following security controls are in place up to date:

- Writing and maintaining the written standards and guidelines for protecting unauthorized access to protected data
- Staying up to date on the applicable laws and regulations
- Performing at minimum annual internal audit of the program
- Have written training guides and forms to document when training is performed
- Training responsible parties on their roles and responsibilities
- Training stakeholders on the applicable key aspects of the program
- Ensuring written program complies with our breach and incident notification and response plan

Section 6: Ensuring Compliance

At the time of this document draft there is no one universal data protection regulation active in the United States of America. However, there is commonality among the leading data protection regulations such as FACTA, GLBA, HIPAA, and HITECH and our program is designed to comply with the provisions common in all of the current data protection regulations by taking reasonable approaches to protecting unauthorized access to protected and confidential data.

Our data disposition program is also designed to meet the requirements of the GDPR data protection regulations which has requirements for any company collecting EU citizen information.

The following is the methodology behind the compliance of our program.

Written Policies & Procedures:

All data protection regulations such as FACTA, GLBA, HIPAA, HITECH require we have written policies and procedures for how to protect unauthorized access to protected data such as PII and PHI.

Our written procedures and policies include our requirements including but not limited to the following.

- Vendor due diligence and sourcing requirements
- Contracting requirements
- Physical and logical security requirements
- Employee training and accountability
- Incident management, breach response plan and corrective action

The contents of this program serve as the written policies and procedures for how our organization reasonably performs data disposition in a secure and responsible manner.

Our incident management, breach response plan and corrective action policies and procedures are documented separately in the NAME DOCUMENT HERE.

Additional employee training policies and procedures are documented separately in the NAME DOCUMENT HERE.

Additional security policies and procedures are documented separately in the NAME DOCUMENT HERE.

Employee Training Program:

Employees must be trained on the policies and procedures to ensure the written policies and regulatory guidelines for protecting unauthorized access to data is achieved. It is unreasonable to expect compliance and to have a program perform well without the formal training of our employees.

Training of our responsible parties occurs regularly and at minimum training is reviewed yearly. The training of employees is documented, and the records are kept by the program's compliance officer.

Assign Employee Accountability:

Assigning ownership and accountability of a data protection program is paramount for the program's success and compliance with data protection regulations. Person(s) assigned with

accountability are expected to respond to incidents, track success, write and implement corrective actions, and act as point of contact with auditors or investigators.

The responsible parties and stakeholder associated with the data disposition program and activities are named in this document.

Vendor Selection & Routine Due Diligence:

Due diligence is required to be done and performed when sourcing a vendor for data disposition services, and routine due diligence is required for any active data disposition vendors.

It is the contracting agent's responsibility to understand and formally approve of a vendor's policies, methods, and procedures including but not limited to breach notification systems, training programs, third party certifications and management systems. These vendor agreements and systems should have routine due diligence and documented no less than once a year.

The methods for performing vendor due diligence for vendor's that perform asset and data disposition are detailed in this document. The parties responsible for vendor due diligence are named in this document.

Contracting Data Disposition Providers:

Any downstream data vendor, disposal, or data destruction providers our organization utilizes is required to be contracted with a formal Master Service Level agreement. The agreement needs to include the vendor's responsibilities to protect data from unauthorized access.

GLBA, and HIPAA both require such an agreement for data protection regulatory compliance. Although other regulations like FACTA do not explicitly require this type of agreement be in place, it is reasonable to assume a contract is a necessary measure required to protect data, confirm and effectively implement written policies and procedures, and protect our organization from the liabilities associated with a non-compliance or data breach.

The requirements for contracting vendors to perform asset and data disposition are detailed in this document. The parties responsible for contract approval are named in this document.

Section 7: Tracking Assets & Disposal Events

It is in our organization's best interest to be diligent when tracking the retirement, disposal, and destruction of our surplus assets to ensure security, compliance, and financial performance of the program.

In the simplest terms tracking disposable assets means knowing what assets have been retired, shipped out for disposal, and confirming the disposal vendor has received and properly processed these assets through our reconciliation process.

Furthermore, all disposal activity and events must be documented in compliance with our program standards and regulatory requirements.

Retirement of Assets:

Retirement of assets must follow the protocol of our applicable asset management program (*reference any other applicable asset program documents here*). When assets are retired the serial number, asset tags, and *any other required asset management information entered here* must be recorded and provided to the responsible party and program stakeholders for approval.

A formal sign off and approval process must be followed before initiating and performing the disposal of any IT assets or data containing devices.

The approval process includes but is not limited to the following:

- Review of assets for reasonable reuse inside our organization by stakeholder
- Confirmation that assets are appropriate for disposal by stakeholder on the basis they are non-functional, obsolete, or otherwise no longer serve a business purpose
- Review of assets to determine and confirm data security and data destruction requirements
- Confirmation of the accuracy of the inventory pending disposal
- Confirmation that assets have been enrolled or otherwise deprovisioned from our registry and/or third-party management tools
- Confirmation that assets have been cleared of any firmware, iCloud, or similar password locks
- Confirmation and approval from stakeholder(s) of the financial obligations associated to project including any projected value returns from service provider

Disposal of Assets:

Equipment approved and designated for disposal should be tagged and labeled appropriately for release to the disposal vendor.

During the physical disposal event the designated equipment for disposal and only the designated equipment for disposal should be released to the vendor. It is the responsible party's duty to ensure an accurate hand-off of equipment to the vendor.

While removing or destroying assets on-site the vendor must perform the appropriate inventorying of equipment according to service level agreements and provide appropriate paperwork, sign off sheets, bill of lading or otherwise equipment manifests, and confirmation of work performed.

Confirmation & Reconciliation of Assets:

Disposed of equipment needs to be confirmed and the disposal reports provided by the vendor reconciled with our data. The responsible party is tasked with reconciling the reports from the disposal vendor with our asset management data.

In any case of failure to reconcile a disposed of asset(s) a reasonable investigation should be undertaken by the responsible party. At the completion of the discovery phase of an investigation (once the problem is fully known) all responsible parties and stakeholders should be notified to determine what, if any, incident response, breach procedure, and breach notifications are required.

When initiating a disposal of equipment, the basics and sample specs of information should be supplied to the vendor so the vendor can accurately account for the supplies and resources needed. However, do not share the complete list of serial numbers or asset management data with the vendor.

Our vendor will be required to supply a list of received and processed assets by serial number and asset tag. If the vendor is given the serial numbers ahead of the service, the integrity of our reconciliation is diminished.

Tracking Disposal Events:

The responsible party is tasked with keeping records of all completed disposal and data disposition events.

At minimum, a record of the following should be maintained and reconciled against the vendor(s) records for accuracy:

- Date of disposal
- Address of disposal
- Name of vendor(s)
- Name of responsible party that performed disposal
- Serialized / asset tag list of equipment disposed of

- Signed shipping paperwork, BOL, or digital signed BOL from vendor
- Any purchase orders, quote numbers or other related financial documents

Section 8: Coordinating On-Site Activities

It is our goal to minimize the impact to our business, stakeholders, and interested parties when performing and coordinating the disposal or data destruction services at our site(s). With this in mind, the responsible party is tasked with ensuring coordination and services provided by our disposal vendor(s) is performed professionally, orderly, safely, and with limited environmental impact.

Scheduling Collection and On-Site Service Events:

The responsible party is tasked with scheduling IT and data disposition collections and services with the service provider(s) in a manner that will be efficient for all parties.

The vendor should be supplied with all pertinent information in order to effectively provide services including but not limited to:

- Any physical obstacles such as stairs, closed ramps, or construction happening at our site
- Our site's security and access requirements such as COI / Insurance proof approval process of the building, scheduling of elevators, or building and security pass process for movers
- A description of the loading requirements, dock hours, or loading zone restrictions
- A reliable point of contact cell phone number or means of paging
- A detailed inventory of the equipment including the quantity of equipment by product type
- Details and photos of any heavy-duty equipment (for example: large copiers, UPS equipment) that may require additional labor to pick-up, pack, or otherwise move
- Description of any additional services that may be required such as de-racking, cable mining, rack removals, or any other activity that may require tools, specialty moving equipment or additional labor resources

Preparing Equipment for Disposal:

The responsible party is tasked with making sure the equipment is physically prepared and available for access by the disposal vendor.

The following steps should be taken to ensure a seamless disposal of equipment:

- Confirm all asset management tracking and approval processes for disposal of equipment has taken place
- Make sure a point of contact with access to the equipment is available to escort the vendor during the scheduled window of service
- Do not schedule disposal events during other business critical service events that may interfere with coordinating the disposal
- Collect and consolidate equipment into designated area(s) that are accessible to carts, pallets, or dolly equipment the vendor will need to use the day of service
- Ensure all scheduling and approvals with the building or facility management has taken place
- Ensure the vendor has confirmed an appropriate time and day for the services and has committed to a reasonable working window for services

During On-Site Services:

The responsible party is tasked with ensuring the activity and vendor's performance while at our location is safe, secure, and does not interrupt normal business or otherwise impact our interested parties.

The following guidelines should be followed by all parties:

- The vendor should be escorted by a responsible party at all times
- Vendor should be met and provided access to equipment & project in a timely manner
- Elevators, hallways, and other public areas should be kept as open as possible
- Media and equipment should never be left unattended unless in a locked secure area designated for storage or on the vendor's locked truck
- Vendor should follow all health & safety and security protocols
- Vendor should follow all building access, parking, and loading zone policies
- The building, fixtures, floors, or otherwise should be protected from damages
- Vendor should inventory and perform on-site services in accordance with agreed upon service levels
- Assets should be handled, packed, and moved with care to reduce damages that can affect our financial returns as well as negatively impact the environment
- Any performance issues, accidents, security incidents, breach incidents or otherwise should be promptly reported to the responsible parties, stakeholders, and vendor as applicable
- Vendor should perform quietly, professionally, and follow directions
- Any activity that appears to be a risk to health and human safety should be immediately reported to the responsible parties, stakeholders, and vendor as applicable.

Section 9: Finalizing ITAD Projects & Report Management

In addition to the tracking guidelines previously provided in this document, steps should be taken to ensure the proper closing and finalization of IT disposal and data disposition projects.

These steps should include the following:

- In addition to the vendor's requirement to store reporting on an accessible platform we are also required to back-up a digital record for the disposal inventory, applicable reporting, and certificates of destruction from the vendor(s) in the appropriate designated location
- Submitting any applicable invoices to the responsible accounts payable party
- Confirm services provided, including but not limited to data destruction service levels meet compliance and security requirements set forth in the vendor agreement
- Directing any applicable payments from the vendor to the responsible accounts receivable party
- Documenting any incidents, complaints, incident/complaint responses, notifications, and/or corrective actions in the appropriate designated location
- Perform applicable asset management processes to finalize the removal of confirmed disposed of assets from our inventory
- Report finalization of project to the appropriate responsible party and stakeholders
- Stakeholders to confirm all necessary asset tracking and asset management guidelines are met as previously described in this document.