ASSET MANAGEMENT POLICY

NextGen CGI, LLC

Document Owner: NextGen CGI, LLC
Effective Date: January 1, 2021
Updated:

NextGen CGI, LLC Asset Management Policy							
Effective Date:				**Document Owner:**			
Revision History							
Revision	Rev. Date	Description	Prepared By	Reviewed By	Date	Approved By	Date
1.0	01/01/2021	Policy	S. Hall	S. Hall	01/01/2021	S. Hall	01/01/2021

1. Overview

Asset management is the process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up to date inventory and asset controls to ensure computer equipment locations and dispositions are well known. Lost or stolen equipment often contains sensitive data. Proper asset management procedures and protocols provide documentation that aid in recovery, replacement, criminal, and insurance activities.

2. Purpose

This policy provides procedures and protocols supporting effective organizational asset management, specifically focused on electronic devices within the organization.

3. Scope

This policy applies to all Company officers, directors, employees, agents, affiliates, contractors, consultants, advisors or service providers that possess or manage assets owned by the organization. It is the responsibility of all the above to familiarize themselves with this policy and ensure adequate compliance with it.

4. Policy

4.1 Asset Types

The following minimal asset classes are subject to tracking and asset tagging:

- Desktop Workstations
- Laptop Mobile Computers
- Tablet Devices
- Printers, Copiers, Fax Machines, and Other Peripheral Devices
- Handheld Devices
- Scanners
- Servers
- Network Appliances (e.g. Firewalls, Routers, Switches, Uninterruptible Power Supplies (UPS), Endpoint Network Hardware, and Storage)
- Private Branch Exchange (PBX) and Voice over Internet Protocol (VoIP) Telephony
- Internet Protocol (IP) Enabled Video and Security Devices
- Memory Devices

4.2 Asset Value

Assets which cost less than $100 shall not be tracked, including computer components such as smaller peripheral devices, video cards, keyboards, or mice. However, assets that store data, regardless of cost, shall be tracked either as part of a computing device or as a part of network attached storage. These assets include:

- Network Attached Storage (NAS), Storage Area Network (SAN), or other computer data storage
- Temporary storage drives
- Tape or optical media with data stored on them including system backup data

4.3 Asset Tracking Requirements

The following procedures and protocols apply to asset management activities:

- All assets must have an internal asset number assigned and mapped to the device’s serial number

- An asset-tracking database or system shall be created to track assets. It shall minimally include purchase and device information including:
  - Data of Purchase
  - Make, Model, and Descriptor
  - Serial Number
  - Location
  - Type of Asset
  - Owner
  - Department
  - Purchase Order (PO) Number
  - Disposition

Prior to deployment, assigned staff shall assign an ID to the asset and enter its information in the asset tracking database or system. All assets maintained in the asset tracking database inventory shall have an assigned owner that is responsible for updating the associated asset information on a defined schedule.

4.4 Asset Disposal and Repurposing

Procedures governing asset management shall be established for secure disposal or repurposing of equipment and resources prior to assignment, transfer, transport, or surplus.

When disposing of any asset, sensitive data must be removed prior to disposal. Assigned support staff shall determine what type of data destruction protocol should be used for erasure. Minimally, data shall be removed using low level formatting and degaussing techniques. For media storing confidential or personally identifiable information (PII) that is not being repurposed, disks shall be physically destroyed prior to disposal.

5. Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy. Satisfactory examples of evidence and compliance include:

- Current and historical asset management system checks for various classes of asset records.
- Spot checks of record input and accuracy against the tracking database.
- Evidence of internal processes and procedures supporting this policy for compliance with general workstation computing policies.

6. Enforcement

Staff members found in policy violation may be subject to disciplinary action, up to and including termination.

7. Distribution

This policy is to be distributed to all staff responsible for hardware and device support.

8. Related Standards, Policies, and Processes

- Removable Media Policy
- Change Management Policy
- Usage Policies
- Audit and Accountability Policy
- System and Service Acquisition Policy

9. Definitions and Terms

The following definitions are not all-inclusive and should be updated as new information is made available:

Term	Definition