Title 2. Employment – Chapter 215
TECHNOLOGY RESOUCES LAW
Rule #003 – Asset Management

3.1 Purpose and Authority
3.2 Adoption, Amendment and Repeal
3.3 Definitions
3.4 Asset Management
3.5 Enforcement
3.6 References

3.1 Purpose and Authority

3.1-1. *Purpose*. The purpose of this rule is to establish a comprehensive framework for the effective management, tracking, and security of Information Technology assets within the organization. This ensures the protection of sensitive data, compliance with applicable laws and regulations, and the efficient use of technology resources to support the mission and operations of the Nation.

3.1-2. *Authority.* The Technology Resources law delegates rulemaking authority to the Digital Technology Services Department pursuant to the Administrative Rulemaking law.

3.2. Adoption, Amendment and Repeal

3.2-1. This rule was adopted by the Oneida Business Committee in accordance with the procedures of the Administrative Rulemaking law.

3.2-2. This rule may be amended or repealed by the Digital Technology Services Department and/or the Oneida Business Committee pursuant to the procedures set out in the Administrative Rulemaking law.

3.2-3. Should a provision of this rule or the application thereof to any person or circumstances be held as invalid, such invalidity shall not affect other provisions of this rule which are considered to have legal force without the invalid portions.

3.2-4. In the event of a conflict between a provision of this rule and a provision of another rule, internal policy, procedure, or other regulation; the provisions of this rule shall control.

3.2-5. This rule supersedes all prior rules, regulations, internal policies or other requirements relating to Information Technology Asset Management.

3.3. Definitions

3.3-1. This section shall govern the definitions of words and phrases used within this rule. All words not defined herein shall be used in their ordinary and everyday sense.

(a) "Active discovery tool" means a tool used to identify devices connected to the network.

(b) "Asset disposal" means the process of securely removing sensitive data from an asset before disposal, based on the data's sensitivity level (Public, Sensitive, Confidential).

(c) "Asset media" means small memory storage assets tracked by Data Owner rather than location, including CD/DVD disks and portable storage devices (USB flash drives).

(d) "Asset tracking database" means a system used to track assets, including all information from the Asset Transfer Form and the date of asset change. It shall be maintained, accurate, and up-to-date.

Commented [CL1]: Definitions should be in alphabetical order

(e) "Asset transfer checklist" means a form filled out by the Data Owner and approved by an authorized representative when an asset is transferred. It includes details such as asset type, ID number, asset name, description, current and new locations, and data owner.
(f) "Asset types" means categories of devices that shall be tracked, including desktop workstations, firewalls, handheld devices, mobile computers, electronic storage devices, printers, copiers, fax machines, multifunction machines, routers, scanners, servers, software (application and operating system), and network switches.
(g) "Asset value" means the cost threshold for tracking assets.
(h) "Data owner" means the person responsible for an asset, typically the most common user for workstations or the primary person responsible for maintenance or supervision for other equipment.
(i) "Digital security office" means the area responsible for approving technology used to erase confidential data to ensure it is not readable.
(j) "DTS" means Digital Technology Services.
(k) "Enterprise software" means software used to configure systems to allow the use of small storage devices on specific Information Systems.
(l) "Resource owners" means individuals responsible for checking the Database regularly to ensure all applicable assets are included.
(m) "Software inventory tools" means tools used to identify and classify operating system and application software on devices.
(n) "Storage device data owner agreement" means an agreement signed by staff to handle portable storage devices and CD/DVD disks responsibly and in accordance with the rule.
(o) "Supported software" means software applications and operating systems currently supported and receiving vendor updates, which are added to the Database.
(p) "Unauthorized assets" means assets not approved or tracked by the organization, which shall be removed, quarantined, or updated in the inventory.
(q) "Unsupported software" means software that is no longer supported, which shall be removed or classified as unsupported in the database.

3.4. Asset Management

3.4-1. Asset Types

. The following devices shall be tracked if they meet the rule requirements:

(a) Desktop workstations;
(b) Firewalls;
(c) Handheld devices;
(d) Mobile computers;
(e) Electronic storage devices;
(f) Printers, copiers, fax machines, multifunction machines;
(g) Routers;
(h) Scanners;
(i) Servers;
(j) Software (application and operating system); and
(k) Network switches.

3.4-2. *Asset Value*

. Assets with a value below a certain threshold set by Accounting shall not be tracked. However, all data-storing assets shall be tracked, including:

Commented [CL2]: Use the word shall and not must. Shall means it's a requirement to do - may means its optional

Commented [SH3]: Format

(a) Hard drives;
(b) Temporary storage drives;
(c) Data tapes (including system backups); and
(d) Other storage devices like CD/DVD disks and USB flash drives are covered for disposal and secure storage purposes.

3.4-3. *Asset Media*.

(a) Small memory storage assets are tracked by the data owner, not location. Enterprise software should configure systems to allow specific Information Systems to use these assets, including:

(1) CD/DVD disks; and
(2) Portable storage devices (USB flash drives).

(b) If permitted for staff, the data owner or area supervisor shall authorize these devices. Staff shall handle these devices responsibly and follow the following guidelines:

(1) Do not place sensitive data on them without authorization. If sensitive data is placed, obtain special permission and keep the device secure.

(2) Do not use these devices to transport executable programs from outside the network without authorization and scanning with approved anti-virus and malware scanners. Only use programs on the DTS department's approved list.

(3) Staff shall sign the storage device data owner agreement, agreeing to handle these devices per rule. This form is submitted when staff begin working with the Nation's data or receive portable storage devices or data backup drives.

3.4-4. *Asset Tracking Requirements*.

(a) All assets shall have a unique identifier, such as an internal tracking number or a manufacturer-provided ID and a means to track them.

(b) An asset tracking database shall track assets, including all information from the Asset Transfer Form and the date of asset change.

(c) The asset tracking system shall be maintained, accurate, and up-to-date, including all hardware and software assets, whether connected to the network or not. Unauthorized assets shall be removed, quarantined, or updated in the inventory. When an asset is acquired, it will be assigned an ID and added to the asset tracking system.

(d) All assets shall have an assigned owner.

(e) Supported software applications and operating systems shall be added to the database.

(f) Unsupported software shall be removed or classified as unsupported.

3.4-5. *Transfer Procedure*.

(a) When an asset is transferred, the data owner shall complete an asset transfer checklist and obtain approval from their supervisor or designated approver. The data owner is responsible for the asset. For workstations, this is typically the primary user. For other equipment, it is the individual responsible for its maintenance or oversight.

(b) The data owner shall complete the asset transfer checklist, indicating if the asset is new, moving to a new location, being transferred to a new data owner, or being disposed of. The following information shall be included on the asset transfer checklist:

(1) Asset Type
(2) ID number;
(3) Asset Name:
(4) Asset Description;
(5) Current Location;

(6) Designated Data Owner;
(7) New Location;
(8) New Data Owner; and
(9) Locations of Sensitive Data.

(c) *Approval*. Once completed and signed by the data owner, a designated representative shall sign the form.

(d) *Data entry*. The completed form is given to the database manager, who ensures the information is entered into the database within one (1) week.

(e) *Database*. An active discovery tool shall identify devices connected to the network. Software inventory tools shall classify operating system and application software. The database shall be updated based on these tools' results. Automated tools shall update the database where possible. Resource owners shall regularly check the database to ensure all applicable assets are included.

3.4-6. *Asset Transfers*.

(a) This rule applies to any asset transfers, including:
(1) Asset purchase;
(2) Asset relocation;
(3) Change of asset data owner (e.g., when staff leave or are replaced); and
(4) Asset disposal.

(b) In all cases, the asset transfer checklist shall be completed.

3.4-7. *Asset Disposal and Repurposing*.

(a) Procedures for secure disposal or repurposing of equipment and resources shall be established before tenant assignment or jurisdictional transport.

(b) Sensitive data shall be removed before asset disposal. The user's manager shall determine the data's maximum sensitivity level.

(c) Actions to be made based on data sensitivity:
(1) *Public*. No requirement to erase data, but normally erase using any means (e.g., reformatting or degaussing).
(2) *Sensitive*. Erase data using any means (e.g., reformatting or degaussing).
(3) *Confidential*. Erase data using approved technology to ensure it is unreadable, as approved by the Digital Security Manager.

3.5. Enforcement

3.5-1. Any staff member found to have violated this rule may be subject to disciplinary action, up to and including termination.

3.6. References

3.6-1. References include:

(a) COBIT APO01.06, APO09.03, BAI09.01, BAI09.02-03, DSS04.07, DSS05.04-05, DSS06.06
(b) GDPR Article 25, 32
(c) HIPAA 164.308(a)(1)(ii)(B)
(d) ISO 27001 A.5.17, A.8.3-5, A.8.18
(e) NIST SP 800-37 3.1, 3.3
(f) NIST SP 800-53 CM-8, PL-4
(g) NIST Cybersecurity Framework ID.AM, PR.PT, DE.DP-2, DE.CM-1-2, RS.RP-1

Commented [CL4]: Who are the authorized representatives?

Commented [SH5]: This should be on all but IAW HR Personnel policies

(h) PCI 1.1.2

End.

Original effective date: [add effective date established by authorized entity] (Certified by LOC on)