


Policy Title:		Asset Management Policy	
	OFFICE OF CHIEF INFORMATION OFFICER	Category	Information Technology Services (ITS)
		Administrative Policy #	
		Revision #	N/A
		Review Frequency	As Needed – no less frequently than triennially
Administrative Division	Information Technology Services (ITS)	Reviewed By	Chief Information Officer
BOWC Approval		Last Reviewed/Update Date	
Implementation Date			

1. OBJECTIVES

- 1.1. To describe requirements for IT asset management related to IT hardware. ITS follows best practice and industry standards to ensure all policies and procedures address the appropriate risks and controls.

2. PURPOSE

- 2.1. This policy establishes the business rules and guidelines for consistency and compliance in managing IT hardware throughout all lifecycle phases of an IT asset.

3. DEFINITIONS

- 3.1. “IT hardware” means the physical aspect of information technology, such as computers, laptops, tablets, smartphones, printers, keyboards, copiers, etc.

4. SCOPE

- 4.1. This policy applies to all employees and contractors/vendors that are or will be involved with using IT hardware. This should be used in conjunction with other DWSD ITS policies.

5. RESPONSIBILITIES

5.1. Chief Information Officer (CIO)

- 5.1.1. The Chief Information Officer (CIO), or delegate, is responsible for publishing this policy and updating this policy as necessary.
- 5.1.2. The CIO, or delegate, is responsible for interpreting and enforcing this policy.

5.2. Information Technology Services (ITS)

- 5.2.1. ITS is responsible for monitoring IT assets.
- 5.2.2. Additional responsibilities are defined throughout the policy section.

6. POLICY

6.1. Purchasing.

- 6.1.1. Refer to the Hardware, Software, and IT Procurement Policy for compliance related to the procurement of IT assets.

6.2. IT Asset Inventory.

- 6.2.1. ITS is responsible for tracking and recording all IT hardware using an asset management application, including the lifecycle of an asset from purchase to retirement to disposal, as well as whom the equipment is issued to and any other relevant information.
- 6.2.2. All other DWSD divisions are responsible for reporting to ITS any IT hardware currently utilized and requesting future IT hardware needs.
- 6.2.3. ITS will assess current IT asset inventories and usage to establish controls to ensure maximum use of IT hardware.
- 6.2.4. All other DWSD divisions are responsible for notifying ITS of any change in location or custodianship of IT hardware.
- 6.2.5. ITS will be responsible of recording any change in location or custodianship of IT hardware within the asset management application.
- 6.2.6. IT hardware will be stored in a secure location and monitored as deemed necessary by ITS.

6.3. Deployment

- 6.3.1. ITS is responsible for tracking and storing any excess IT hardware.
- 6.3.2. All other DWSD divisions will be responsible for requesting IT hardware for new employees, contractors, and vendors.
- 6.3.3. IT hardware will be stored in a secure location when not in use and monitored as deemed necessary by ITS.
- 6.3.4. ITS will ensure that equipment is fully configured and ready for use.
- 6.3.5. IT hardware will be deployed with encryption enabled by default and to specific individuals or a specific location.
- 6.3.6. Refer to the User Account Management Policy for additional guidelines.

6.4. Maintenance

- 6.4.1. ITS is responsible for maintaining all IT hardware and ensuring it meets business needs and customer expectations.
- 6.4.2. ITS will ensure that IT hardware is receiving timely patches, is securely configured, and maintains version control.
- 6.4.3. ITS will monitor IT hardware for maintenance needs and performance, management of refresh cycles, information management, asset valuation, and continuous assessment of the hardware's use and functionality.

- 6.4.4. ITS will determine, on a regular basis, if IT hardware should be maintained, modified, rehabilitated, find an alternative use for, or disposed.

6.5. Retirement and Disposal

- 6.5.1. ITS is responsible for providing planned, orderly, and secure disposition of assets.
- 6.5.2. This includes proper de-installation and determination of disposal, replacement, renewal, or redeployment.
- 6.5.3. Disposal may include a sale, transfer, donation, write off, or recycling. ITS will make this determination in the best interest of DWSD.
- 6.5.4. Only ITS may dispose of IT hardware.
- 6.5.5. IT hardware must have all software and information securely removed prior to disposal.
- 6.5.6. Highly sensitive data must be deleted using secure methods as soon as the information is no longer required.
- 6.5.7. Any media storage of data, such as disks, must be physically destroyed prior to disposal.
- 6.5.8. Human Resources is responsible for notifying ITS when an employee is being terminated to ensure all IT hardware can be collected in a timely manner. Departments/Divisions should notify ITS when a vendor or contractor is being terminated.
- 6.5.9. Refer to the User Account Management policy for additional information.

6.6. Employee and Contractor/Vendor Use

- 6.6.1. DWSD employees, contractors and vendors may not remove IT hardware from company premises except those that are assigned to them, such as laptop, tablet computers, smartphones, etc.
- 6.6.2. IT hardware should only be removed for teleworking and work that is outside of the office that is a part of an assigned position.
- 6.6.3. DWSD employees, contractors, and vendors are responsible for safeguarding any IT hardware removed from the building, including keeping the hardware under their direct physical control whenever possible and physically securing the hardware when this is not possible.
- 6.6.4. DWSD employees, contractors, and vendors must immediately report the loss or theft of any IT hardware to the ITS. A police report should be completed and provided to the CIO in a timely manner.
- 6.6.5. DWSD employees, contractors, and vendors are not allowed to bring personal IT hardware into work locations with the purpose of connecting to the firm's private network and data.
- 6.6.6. IT hardware and data assets are the property of DWSD and must be returned upon termination or voluntary separation.
- 6.6.7. IT hardware should not be used by anyone other than the assigned individual(s).

6.6.8. Any exceptions to this policy must be requested and approved by ITS and document the business/technical justification and the duration of the exception.

6.6.9. Refer to the Information Security Policy for additional guidelines.

6.7. Network Storage

6.7.1. Onsite servers will be locked in a separate room and only a select few approved DWSD employees will have access. Activity monitoring and environmental controls will be utilized to monitor the server room.

6.7.2. Granting and terminating access to the server room will follow the same procedures as defined in the User Account Management policy.

6.7.3. The list of those with access to the server room will be reviewed annually and any changes made documented in the ticketing system.

6.7.4. Virtual servers, located offsite, will only be accessible by a select few approved DWSD employees. Controls will be in place to monitor access to virtual servers.

6.8. Reasonable and Necessary Accommodations

6.8.1. Management may take reasonable and necessary actions to accomplish the intent of this policy.