

Printer Management Standard

Introduction

This standard defines the policies and technical requirements for deploying, configuring, securing and maintaining printers across the organization's network. It establishes consistent practices to minimize downtime, protect sensitive information and reduce unnecessary printing and resource usage.

By following this standard, the IT team ensures all printing resources are:

- Properly secured against unauthorized access.
- Optimally configured for network performance and user accessibility.
- Centrally managed for better visibility and reporting.
- Compliant with industry best practices and regulatory obligations.

This standard applies to all networked printing devices, including multifunction printers (MFPs), dedicated print servers and any print-enabled endpoints on the corporate network, whether physical or virtual.

Purpose

To establish a consistent, secure and efficient approach to managing network-connected printers across the organization. This standard ensures proper configuration, usage, maintenance and security of all print devices.

Definitions

Dynamic Host Configuration Protocol (DHCP) – a network management protocol used to automatically assign IP addresses and other network configuration settings (such as subnet mask, default gateway and DNS servers) to devices (clients) on a network.

Mobile device management (MDM) – a set of technologies, policies and tools used by IT administrators to securely manage, monitor and control mobile devices – such as smartphones, tablets and laptops – across an organization.

SMB printing – the method of printing over a network using the server message block (SMB) protocol – a file sharing protocol primarily used by Microsoft Windows systems.

Standard

Printer protocol standards.

Protocol	Description	Use Case
IPPS (IPP over HTTPS)	Secure printing via HTTPS	Default for all modern printers
IPP (Internet Printing Protocol)	Standard printing protocol over HTTP	For internal, non-sensitive use
JetDirect (Port 9100)	Raw socket printing	Legacy or specific device needs
LPD/LPR	Unix-based print service	Legacy systems only
AirPrint	Driverless printing for Apple devices	Mobile and BYOD environments

SMB printing may be permitted for Windows-only environments with proper security controls.

Printer deployment guidelines.

- All printers must be deployed with DHCP reservations.
- Printers should be named using a standard format: **Agency-Location-Model-AssetTag or Last 5 of Serial** (e.g., GOV-NYC-Floor2-HP4050-12345).
- Printers must be connected only to designated VLANs/subnets for printing through hardwired connections, either network Ethernet connection or direct to computer through USB.

Driver and print server management.

- All drivers must be approved and provided by IT.
- Use universal print drivers where possible (e.g., HP Universal, Ricoh Universal).
- All printers must be managed via a centralized print server or print management platform.
- End users are not permitted to install network printers directly through IP address.

Access control.

- Use group policy (Windows) or MDM (macOS/iOS) to assign printers based on user roles or departments.
- Secure printing (PIN or badge release) must be enabled on multifunction devices (MFDs) or high-volume devices.

Decommissioning and disposal.

- Remove all stored print jobs and configuration data.
- Pull hard drive for destruction.
- Perform a factory reset before recycling or decommissioning.
- Confirm device disposal through approved e-waste vendors.

Printer support responsibilities for agency-owned devices.

- OMES provided support:
 - Network connectivity.
 - Printer naming and configuration.
 - Scanning setup.
 - Ensuring staff can successfully print to the device.
- Agency ownership:
 - Routine maintenance and mechanical upkeep.
 - Adding or replacing toner.
 - Clearing paper jams.
 - Replacing worn rollers.
 - Addressing print quality, imaging or alignment issues.
 - Handling mechanical or hardware malfunctions.
 - Any other consumable or wear-related maintenance.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

Rationale

To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 09/15/2025	Review cycle: Annual
Last revised: 01/05/2026	Last reviewed: 01/05/2026
Approved by: Dan Cronin, Chief Information Officer	