Administrative Policy #: 1302
Title: Printing Standards
Effective Date: January 20, 2026

SECTION 1. PURPOSE & SCOPE

1.1. PURPOSE: This administrative policy is designed to safeguard the confidentiality, integrity, and availability of printed documents at Fairmont State University. It outlines the standards for secure printer usage and ensures appropriate access, authentication, and support across University-owned printing devices.

1.2. SCOPE: This administrative policy applies to all members of the Fairmont State University community, including faculty, staff, and students, and governs the usage of University-provided and personal printing devices. The administrative policy encompasses access control, usage standards, security requirements, environmental considerations, and compliance expectations.

SECTION 2. APPROVAL, DELEGATION & APPLICABILITY

2.1. AUTHORITY: The Chief Information Officer (CIO) has the authority to implement, enforce, and grant exceptions to this administrative policy.

2.2. DELEGATION: The CIO may delegate operational responsibilities to Information Technology Services (ITS) staff for implementation, monitoring, and maintenance. Delegated authority does not extend to exceptions unless explicitly authorized by the CIO.

2.3. APPLICABILITY: This administrative policy applies to all University employees, students, contractors, and affiliates who use or manage printing resources within Fairmont State University, whether through University-provided printers or personal devices within University premises.

SECTION 3. DEFINITIONS

3.1. AVAILABILITY**:** Ensuring that printing resources and documents are accessible when needed

3.2. CONFIDENTIALITY: Ensuring that printed documents are only accessible to authorized individuals

3.3. DIRECT PRINTING: Sending a print job directly to a printer without going through a print server

3.4. INTEGRITY: Maintaining trustworthiness and accuracy of information throughout its lifecycle

3.5. PERSONAL PRINTER: A printer not part of the IT vendor contract or supported by the University

3.6. VENDOR PRINTER: A printer provided and supported by an external supplier under contract with IT Services

SECTION 4. POLICY

4.1. POLICY: It is the policy of Fairmont State University that access to University printers, located on campus or within the residence halls, is restricted to authorized users through secure authentication methods, including manual login or card access.

4.2. PURPOSE: University-provided printers must be used primarily for academic and administrative purposes. Personal and non-networked printers for employees are discouraged and not funded.

4.3. PERSONAL DEVICES: Students may use personal printers in residential housing, but these are not supported by IT Services.

4.4. DESTRUCTION: Sensitive documents should only be printed and retrieved when the user is physically present, and discarded documents must be securely destroyed. Secure destruction of a print job refers to rendering the printed document unreadable. This can be accomplished by shredding the physical printout. Documents can also be placed in shred bins located throughout campus.

4.5. RESPONSIBILITY: Departments are expected to promote responsible and secure printing practices.

4.6. RELEASE: Documents sent to University printers will not be released until the authorized user logs in, taps, or swipes their ID to authenticate and release the job.

4.7. The University prioritizes the use of contracted vendor printers for cost efficiency, standardization, and effective support.

SECTION 5. COMPLIANCE

5.1. COMPLIANCE: All users must comply with this administrative policy and any associated University guidelines. Regular training and awareness sessions will be conducted to ensure understanding and compliance.

5.2. NONCOMPLIANCE: Failure to comply with this administrative policy may result in restricted access to printing resources or disciplinary actions. The University reserves the right to audit printing activities. Exceptions to provisions may be granted by the CIO under specific circumstances.

SECTION 6. REVISION HISTORY

6.1. FREQUENCY OF REVIEW: This administrative policy will be reviewed every 3 years or upon significant changes to technology, security practices, or University priorities.

6.2. APPROVED: President Davis approved this policy on January 20, 2026.