

THE UNIVERSITY OF ALABAMA IN HUNTSVILLE

DOCUMENT IMAGING AND STORAGE POLICY

-INTERIM-

Number 02.01.44

Division Office of Information Technology (OIT)

Date August 2015

Purpose The purpose of this policy is to establish standards for the storage of documents within The University of Alabama in Huntsville (UAH) Document Imaging and Storage System.

Policy This policy establishes the practices to ensure adequate storage space, fast retrieval times, and a secure environment for any unit that wishes to utilize the Document Imaging and Storage System. Whenever possible, the central UAH Document Imaging and Storage System shall be used. Exceptions shall be documented and approved by the unit head. All university units utilizing this system will be governed by this policy.

Procedure

1.0 Training

Any unit wishing to use the Document Imaging and Storage System will be required to undergo basic training before access is granted. Training will be provided as part of the implementation process and additionally upon request. OIT will provide retraining as necessary to ensure that staff are updated in regards to any system changes that may occur over time.

2.0 Scanners

Hardware should meet industry standards including supporting the ISIS driver that compresses images after being scanned.

OIT can provide a list of recommended scanners and their specifications upon request. OIT will assist with the configuration of scanners to ensure proper setup.

2.1 Scanner Settings

The industry standard Dots per Inch (DPI) setting for scanning documents is 300 DPI which provides great resolution and a small image file.

2.1.1 Recommended Default Settings

- Black and White (Bi-tonal)
- DPI will always be 300 DPI

2.1.2 Color Scanning

Color scanning should be limited to cases where for legal or readability reasons it is required. If color scanning is necessary, the settings will be 24-bit color at either 100 or 75 DPI; 16-level gray or 256-level gray should not be used.

Settings above industry standards must first be approved by OIT.

3.0 Image

3.1 Access to Images

Access to images will be provided only through the Document Imaging and Storage System Application. Accounts for the system are maintained by OIT and will be administered in conjunction with Banner data credentials.

During the implementation process and when new staff are requested to be provided access, OIT will work with the data steward(s) to establish the application and document level security access.

Access to scanned images will only be granted upon the approval of the data steward(s).

3.2 File Size

In order to conserve storage space and ensure uninterrupted scanning, the size of the final image will be monitored via audit mechanisms. OIT will automatically resize images that exceed established limits and work with the user to adjust configurations as needed.

It may be necessary for the user to delete and rescan image(s) in situations where OIT cannot adjust the file size without compromising the integrity of the image.

4.0 Verification and Retention

4.1 Verification

It is the responsibility of the end user to verify the scanned image and retain the printed document until verified.

4.2 Retention

Documents will be stored in the most efficient way possible. OIT reserves the right to move documents to different storage media if necessary. Advance notification will be provided to users to the extent possible.

4.3 Removal of Documents

Documents are to be removed from the system when they are no longer needed. It is the responsibility of the end user to ensure that the disposal of documents adheres to applicable retention policies and laws.

5.0 Account Revocation

Failure to adhere to the established settings, repeated abuse of the system, and/or failure to act promptly on a notification may result in the temporary suspension of scanning privileges until the settings are properly configured with the assistance of OIT.

6.0 Scanner Setting Quick Guide

Setting	Resolution	DPI
Black/White	Bi-tonal	300
Color	24-bit	100
Color	24-bit	75

NOTE: Only use color setting where necessary for legal or readability reasons.

6.0 Compliance with Policy

Failure to abide by this policy may result in the loss or suspension of IT privileges, claims for reimbursement of damages, disciplinary action, and/or referral to appropriate state/federal law enforcement authorities.

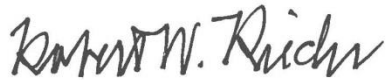
Violations that constitute a breach of the Student Conduct Code, the Faculty Handbook, or the Staff Handbook will be referred to appropriate authorities. OIT personnel may take immediate action as needed to abate

ongoing interference with system or network operations or to ensure integrity of university systems or data.

Review

The UAH Cybersecurity and Policy Advisory Council is responsible for the review of this policy every three years (or whenever circumstances require).

Approval

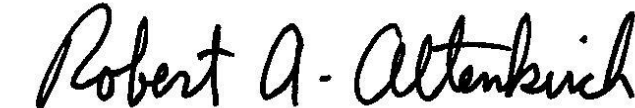


Chief University Counsel



Provost and Executive Vice President for Academic Affairs

APPROVED:



President