

Security Policies and Procedures for University of Missouri Printing Services and Digiprint Centers

Version 1, December 27, 2006

These policies and procedures are put forth to address the security concerns arising in 2006 from variable data processing procedures being added to the list of Digiprint services, as well as the transfer of management of the IATs printing facilities to Printing Services, which results in a portion of their print jobs being diverted to Digiprint's toner-based machinery.

These policies and procedures should be made available for review to any customer upon request.

Policies and Procedures:

Printing Services and Digiprint, and their employees will take appropriate actions and follow appropriate procedures to ensure the security and privacy of all documents and information in our possession which have been designated as sensitive. These include

Protection of sensitive digital data files:

Customers will be encouraged to encrypt and password protect all sensitive digital data being transferred to Printing Services. Printing Services will not store or back-up sensitive data on public servers, limiting storage of sensitive data to one secure machine for the duration of the production of the job.

After the job is printed, the data files will be deleted. If data is manipulated and given back to the customer, it will be encrypted and password protected before it is transferred. These data files will then be deleted.

Protection of printed materials:

Printed materials containing sensitive information will be produced, stored/maintained, processed, handled, delivered and disposed of in a secure manner. Access to these materials by personnel should be limited to those required for the items just mentioned. Specifically, all jobs including sensitive data should be produced only at Printing Services' main plant. A secure room will be used to store printed materials for more than a few hours. Spoilage must be kept separate from general spoilage and disposed of securely. Printed materials containing sensitive data must be delivered to a specific person or secure facility so as to maintain a continuous secure environment. Such materials cannot be "dropped off" or left unattended to any location, unless that location is designated as secure and locked and protected from general access.

Protection of sensitive information in general:

No employee shall view, copy, or transmit sensitive information in any way unless it is required for the production of a specific print job.