

# GCSU

## Information Security Operational Procedures

### Legato Document Imaging

#### BACKGROUND

Document imaging has become a necessary tool to satisfy the need to archive extremely large amounts of paperwork that the University is required to maintain. As protected information is digitized, it becomes necessary to protect it in a manner different than one would protect a tangible paper document. Digital documents must be protected not only at their final storage facility, but at the time of digitization, and during transmission as well. Likewise the controls necessary to protect the electronic documents in their final location are vastly different than those used to protect a filing cabinet, a safe, or a warehouse.

#### SCOPE

This procedure outlines the measures necessary to help ensure the prudent protection of digital documents and specifically applies to the Legato suite of applications including, but not limited to: BannerXtender, ApplicationXtender, and WebXtender. This procedure address the controls necessary to secure to a reasonable measure the data store or file servers used with the Legato applications as well.

This policy is specific to the Legato applications and supersedes any and all other broad policies that may address these systems.

#### POLICY

#### SCANNING STATIONS

A Legato Scanning Station is comprised of a Windows workstation and a SCSI or IEEE 1394 (Firewire) scanner. These workstations shall be for the sole purpose of transferring paper documents to a digitized format and transmitting the documents to an approved storage server.

#### SERVER ACCESS

Ensuring both the functionality of the Legato product and the security of the information housed on Legato data stores, it is imperative that:

- File server direct access shall be for the purpose of system administration and direct upload of documents by scanning stations.
- Direct share access shall be restricted by access control list and monitored by the System Administrators and Network Administrators.
- Share access will be authenticated via individual username and password as assigned by the System Administrator.
- General access to server outside of the scanning stations will be via web interface (WebXtender) and secured within the Legato Application based upon Banner permissions and roles. This is in accordance with the Banner Acceptable Use Policy.
- Web access shall be restricted via firewall and/or routing policies to appropriate subnets or address ranges. Addresses within the designated range for wireless communications shall be denied access.

## **BACK-UP**

The Legato data store shall be mirrored in its entirety and a tape backup shall be kept offsite for the longest duration required by records retention laws or statutes.

## **EMPLOYEE USAGE**

## **APPROVAL**

Access to Legato systems or functions shall be with supervisor approval. Access requests must be submitted in writing by the supervisor on behalf of the employee. Requests shall be submitted to the CIO on a Legato Access Request form. CIO approval shall only be granted provided that there is a documented and proven need for the named employee to be granted access to the Legato systems. Access may be restricted to specific functions by the CIO or supervisor depending upon the needs of the employee to effectively do their job.

## **SUPERVISOR RESPONSIBILITIES**

The supervisor shall be responsible for:

- Monitoring the Legato systems to ensure that they are used appropriately.
- Requesting access for employees.
- Notifying the Division of Information Technology if access to Legato is no longer needed.
- Reporting to the CIO unusual activity or behavior of the Legato systems.
- Providing appropriate training to employees based upon their job function.

Information Technology  
Campus Box 050  
Milledgeville, GA 31061-0490  
(478) 445-1196

Revised: 03/16/09

