Title	Information Technology Protection – Guide to Securing Networked Printers, Scanners, Copiers, and Faxes
Type	Procedure
Category	Security
Effective Date	July 1, 2014
Approved	July 1, 2014
Revised	
To Be Reviewed	July 1, 2016
Parent Policy	Information Technology Protection Policy
Scope	Applies to all Multifunctional printing resources
Policy	**Procedure Definitions:**

The City of Albuquerque Guide to Securing Networked Printers, Scanners, Copiers and Faxes is a reference resource for all CABQ departments that use a networked device (i.e., printer, copier, scanner and fax). In particular, the guide offers recommendations on:

- Securing networked devices against misuse and compromise by unauthorized users.
- Enhancements to existing security measures.

Background:

Securing networked devices is important for a number of reasons:

- Most are simply "plugged-in" to the network, deployed using the minimal settings required to make the device respond and operate.
- Once installed, they rarely receive recommended application and operating system updates and vendor patches.
- Networked devices can be administered via the network; physical access to the device may not be required.
- Due to increased sophistication (built-in "intelligence") and ever-increasing storage capacity, they can be used to launch attacks, store unauthorized data, retrieve scanned and printed documents, and print objectionable or

unauthorized material.

Procedure Provisions:
Recommendations include:

1. The CABQ standards and commodities provides equipment commodities in the purchase of printing equipment. When considering new or replacement acquisitions, contact Information Technology Services Department (ITSD) Service Desk or Purchasing for recommendations and preferred vendors. Select a device that is configurable and offers security features.
2. Review vendor documentation for any listing of security-related features and recommendations on secure installation and implementation. Contact your vendor and inquire about equipment upgrades that include security features.
3. Establish a strong administrator password on the device to help defend against attacks and prevent re-configuration by an unauthorized user.
4. Where the device supports access control lists (ACLs), configure them to block all traffic from outside the City of Albuquerque range (143.120.0.0/16) or further restrict access to only the department subnet. If personnel need access to the departmental printer from off-campus, access should only be permitted using the City of Albuquerque VPN.
5. If there is a FTP server on the printer, turn it off. Similarly, turn off Telnet access if it exists.
6. If SNMP is not required, disable it. Where it is required, change the default SNMP string.
7. Disable the Appletalk and Netware protocols; disable any protocol or service not required.
8. Use hard-drive encryption and automatic deletion or overwrite of data features where offered.
9. Auto-delete and auto-purge capabilities are available on most multi-functional printers (MFP). Capabilities such as HP's Secure Erase provide deletion of print jobs in printer memory. It is critical that printers which are used for sensitive documents utilize auto-delete configuration. Any MFP device with storage capabilities prior to being removed from service should be erased. The manufacturer of the device can assist in configuring auto-delete capabilities.
10. Establish a contact point to receive all notifications

regarding the devices and schedule periodic reviews to help ensure that patches and updates are regularly applied.

11. At times when normal maintenance of equipment is performed, request the vendor's technician to refresh/reformat (where possible) the hard-drive.
12. When transferring, retiring, disposing of or trading-in current equipment, reformat and overwrite the hard-drive (if featured) or contact ITSD Service Desk to assist in these processes.

In all cases, protection shall be provided in compliance with all City information technology policies, standards, procedures and guidelines

Rationale

Information technology protection requires continuous efforts to secure the information systems for critical infrastructure, including emergency preparedness communications, and physical assets that support such systems. Protection of these systems and the data which resides on systems is essential to consistent and effective service delivery.