Computer Data and Media Disposal Policy Introduction

A recent series of news articles highlight privacy issues associated with today's modern multifunction copier devices. Most businesses have them. The devices are all in one digital copiers, scanners, printers and fax machines. These devices have internal hard drives that are often forgotten repositories of all sorts of images. The devices are usually connected to an IT network. Often dedicated network locations store scanned images or faxes, until they are retrieved by a user.

The evolution of the simple copy machine has transformed a “copier” into a digital time-bomb packed with highly-personal or sensitive data. Nearly every digital copier built since 2002 contains a hard drive like a personal computer, storing an image of every document copied, scanned, or emailed by the machine.

Data security kits

Several MFP brands still offer an optional data security kit that provides the following services:

- Encrypts all data prior to being stored in DRAM
- Encrypts all data stored on the hard drive
- DRAM is cleared after copy, scan, fax and print use
- Runs automatically without user initiation
- Provides overwriting routines to make deleted data irretrievable

Sensitive information

Businesses typically enter sensitive information into the MFP’s address book. Names, email addresses and fax numbers are examples. Also, MFPs have the ability to create document servers where employees can save printed, scanned, or copied documents.

Other concerns

- **Physical access**: Think about who has access to the copier; employees, customers and service technicians (genuine and imposters). If sensitive information is stored, it needs to be protected.
- **Network access**: Most MFPs use proprietary operating systems, which makes them fairly immune to exploitation but it is a good idea to check the **National Vulnerability Database** for any problems with your specific brand of MFP.

- **Web-based configuration**: Most MFPs have a web interface for configuration and access to the address book. The interface is usually pass-word protected. Make sure it's not the default password.

- **Public MFPs**: We advise against using any public MFP or copy services like **FedEx Office** if the document to be printed or copied contains sensitive information. It is impossible to know how the MFP is configured and whether it is saving a copy of each digitized document.

Best practices for securing MFPs

One thing became clear during review of various MFP manufacturers considered to offer appropriate security, MFP physical and digital security should be folded into the companys' IT security policy. To that end, please see below what manufacturers consider important:

- **Meet industry certification**: When deciding what brand and model to lease or buy, make sure the device meets industry security standards. Two prominent certifications are **ISO 15408 Level 3 Certification** and **IEEE-2600-2008**.

- **Ease-of-use versus security**: Company management must decide what access controls to use if any. Access controls typically consist of user authentication, account codes and password protection.

- **Data security kits**: MFP distributors need to inform customers about data security packages and their importance. If there are any security concerns, using a data security kit will address them.

- **End-of-Life considerations**: When buying or signing a lease for MFPs, determine what should happen to the hard drive at end-of-life. Typical options are; destroy the hard drive, keep it on-site, or have the MFP distributor or technician scrub the hard drive using an approved process.

DRAFT POLICY TITLE: Computer Data and Media Disposal Policy
DATE DRAFTED: **2/4/2011**
APPROVED DATE: **2/9/2011 by ITAC**
BRIEF DESCRIPTION: Washoe County (County) policy regarding the proper transfer, disposal and/or reuse of computers and other digital storage media.

Introduction:

The County is committed to compliance with federal/state statutes associated with the protection of confidential information as well as ensuring compliance with software licensing agreements. As a result of this commitment, all digital storage devices under County control which contain licensed software programs and/or institutional data must be reliably erased and/or destroyed before the device is transferred out of County control or when being transferred from one division/department to another, except when authorized by department head.

Scope:

All personnel of the County have a responsibility to ensure the confidentiality of federally regulated and otherwise protected sensitive or proprietary information residing on County owned computer systems and other digital storage devices and media.

Affected Devices:

All computers and digital storage devices including, but not limited to, desktop workstations, laptops, servers, notebooks and handheld computer hard drives; external hard drives; multi-function copiers and all external data storage devices such as disks, Storage Area Networks (SAN), optical media (e.g., DVD, CD), magnetic media (e.g., tapes, diskettes) and non-volatile electronic media (e.g., memory sticks), are covered under the provisions of this policy.

Policy Statement:

1. County owned computer and digital storage media must have all institutional data and licensed software reliably erased from the device prior to its transfer out of County control, and/or the media must be destroyed, using current best practices for the type of media. Delete, Remove and Format operating system commands, as well as disconnecting or clipping wires to a drive, **do not** actually erase data from the media and therefore are not acceptable methods for preparing media for transfer or disposal.

2. County personnel will request documentation attesting to the erasure of licensed software and institutional data by an approved IT service provider. Otherwise, they will either perform the erasure of data according to approved procedures prior to release (e.g., sale, donation) of the computer or digital storage media or they will be responsible to destroy the media.

3. The Washoe County Security Team will work with appropriate department technology staff to ensure that procedures consistent with security best practices are followed for the reliable removal of licensed software and confidential data before equipment transfers take place. Otherwise, departments must engage an IT service provider approved by the County Security Team to prepare media for transfer or disposal.

4. Computer and electronic storage equipment identified for title transfer must be reviewed and subsequently cleaned by an IT service provider approved to perform data erasing. Licensed software and institutional data deemed to be the property of the County must be removed prior to title transfer of equipment from the County.

5. Computers, copiers, digital storage media and equipment containing digital storage media, when included as part of a trade-in purchase or end of lease, must be identified on the requisition and subsequent purchase order for new equipment. Documentation attesting to the erasure of licensed software and institutional data by an approved IT service provider will be required in order to complete the purchase. The County must have a non-disclosure confidentiality agreement (NDA) in place with any vendor receiving devices for trade-in, or that must be replaced as part of a warranty or repair contract but which cannot be erased for technical reasons.

6. County employees should not use any public MFP (multi-function printer) or copy services such as **FedEx Office** or Kinko's if the document to be printed or copied contains sensitive information. It is impossible to know how the MFP is configured and whether it is saving a copy of each digitized document.

7. Responsibility for following disposal policy will be based on the purchasing entity and included in all contracts and lease agreements. Smaller purchases (such as thumb drives) will be the responsibility of the individual or department at time of disposal. Transfer of devices to other internal departments is authorized as long as information sharing is not an issue.