

# Computer Disk and Media Disposal Training

Jane Drews  
University IT Security Office  
July 2006

# Agenda

1. Policy review
2. Process and procedure
  - Forms
  - Documentation
3. Wiping guidelines
4. Recommended Tools

# Disposal Policy Review

<http://cio.uiowa.edu/policy/ComputerEquipmentDisposal.shtml>

- Licensed software is removed as appropriate
- Compliance with regulations regarding privacy of information
- Protection of sensitive or proprietary information (within UI and without)

# Disposal Policy Review

- Licensed software and institutional data must be **reliably erased** before a device leaves UI control

OR

- Device/media must be **destroyed**

# Disposal Policy Review - Scope

- All computers and digital storage devices
- Transfer, sales, donation, destruction, title transfer, cannibalizing, trade-ins,  
...



# Disposal Policy Review

- Departments may be approved to
  - prepare devices for transfer within UI, including UI Surplus
  - destroy media
  - prepare devices prior to title transfer

# Disposal Policy Review

- Employ current best practices for preparation of the media
- Comply with UI Equipment Policy

# Process and Procedure: Property Management Office (PMO)

- Both Tagged and Non-Tagged (for now)
- Forms must go to PMO first
  - Review for federal equipment/assets
  - Review for inventory management changes
  - PMO forwards request to Surplus (if applicable) w/i 24 hrs.
- Internal Transfers of UI Equipment  
<http://www.uiowa.edu/~eforms/pm/itue.pdf>
- Surplus Removals <http://www.uiowa.edu/~eforms/pm/srrf.pdf>
- Title Transfers of UI Equipment  
<http://www.uiowa.edu/~eforms/pm/ttue.pdf>
- Off Campus use of Property  
<http://www.uiowa.edu/~eforms/pm/ocup.pdf>

# Policy and Procedure: Org/Dept Records

- Equipment Serial Number
- Description (type, make, model, location, ID/Tag#, owner)
- Date
- IT Staff name
- What was done
- Retain for 6 years



# Wiping Guidelines

The effort undertaken to ensure data is securely removed from media should be in direct proportion to the sensitivity of the data on that media and the risk of exposure.



# Wiping Guidelines

- Public Draft - February 2006 NIST Guidelines for Media Sanitization:  
[http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3\\_2006.pdf](http://csrc.nist.gov/publications/drafts/DRAFT-sp800-88-Feb3_2006.pdf)
  - Types of media and recommendations for disposal/sanitization
  - Sample form for tracking media

# Wiping Guidelines

## Type 1: Low Risk

- Internally shared devices such as checkout laptops
  - Instruct users not to store data locally
  - Consider “Eraser” file-based wipe software
  - Image the machine on a regular basis &/or between lengthy (e.g., travel) uses
- Internally transferred equipment in dept
  - Single pass wipe (depending on the data)
  - Format and load/image

# Wiping Guidelines

## Type 2: Medium Risk

- Transfers of equipment between UI departments (e.g., not leaving UI control)
  - Single pass wipe (depending on the data), or DOD wipe
  - Format and load/image

# Wiping Guidelines

## Type 2: Medium Risk, cont'd

- Disposal of equipment, cannibalizing
  - Wipe not necessary if destroying
- Title Transfers (going to a known entity)
  - Must remove UI licensed software
  - Must remove all confidential data not approved for release (i.e., Research data)

# Wiping Guidelines

## Type 3: High Risk

- Sales, donations, etc (leaving UI Control)
  - Must use DOD standard (3+ pass) for wiping devices (See DOD 5220.22M <http://www.killdisk.com/dod.htm>)
  - Must transfer to Surplus/WiderNet
  - Keep devices in secure location before pickup
  - Mark system (sticker with dept, when, what, who, desc)
  - Surplus may provide recycle/shredding services, and device tracking services in future.

# Wiping Guidelines

## Type 4: Special Cases

- Warranty Service
  - UI-level or individual Confidentiality Agreement (CA) or Non-Disclosure Agreement (NDA) in place with vendor (Office of General Counsel)
- Broken equipment
  - Destroy, shred, degauss media
- Trade-ins
  - DOD Wipe and document on Purchase Order
  - If not possible, negotiate CA/NDA with vendor

# Tools

- Place to keep records (Paper files/forms, Spreadsheet, Access DB, etc)
- Bootable Disk Wipe utility
- Loadable CD/Ghost images of machines
- Stickers to mark wiped machines for UI Surplus (with dept, when, what, who, desc)

# Tools

- Active@Killdisk <http://www.killdisk.com>
- Darik's Boot and Nuke <http://dban.sourceforge.net/>
- Eraser <http://www.heidi.ie/eraser/>
- WipeDrive & MediaWiper <http://www.whitecanyon.com>
- Wipe <http://wipe.sourceforge.net>
- Ghost “gdisk /diskwipe /dodwipe”
- “Secure Empty Trash”
- Knoppix “Shred” <http://www.killdisk.com/dod.htm>

# Questions?

University IT Security Office

[security@uiowa.edu](mailto:security@uiowa.edu)

335-6332