If your building were to burn down today...

Could you re-open for business in another location tomorrow morning?

Records Management’s Charge:

- Protect the Records of the Institution
  - COORDINATE the record retention and disposition of the College
  - MANAGE inactive, occasionally accessed material
  - PROVIDE consulting services to College Departments
  - PLAN for future record keeping needs

Records Management Staff

- Wess Jolley, Records Manager
- Diane Preston, Records Center Supervisor
- Ginger Harrington, Records Management Technician
- Deborah Siwulec, Records Management Technician

Diane Preston, Records Center Supervisor

Ginger Harrington, Records Management Technician

Deborah Siwulec, Records Management Technician

Introductions

- Your Name
- Department
- Job
- Record Responsibilities

The Records Management Training Cycle

- Part 1: Managing Records in an Office Environment (June 2)
- Part 2: Using Records Management Services (June 9)
- Part 3: Vital Records Identification Protection, and Disaster Recovery (Today!)
- Part 4: Introduction to Digital Records (June 23)
- Part 5: Digital Document Management (June 30)

Session Outline for Today

- “What is a Record?”
- The Information Disaster Plan
  - Assess and reduce risks
  - Identify the vital records
  - Break!
  - Protect the vital records
  - Ensure ability to resume and reconstruct
  - Document policies and procedures

Records Management Manual
http://www.dartmouth.edu/~library/recmgmt/
“What is a Record?”

- Any recorded information generated in the course of conducting business, and which must be maintained to meet the fiscal, legal, historical or administrative needs of the organization.
- Records should be declared and classified as part of a formal process or workflow.
- Records exist regardless of their format.

RECORDS:

Are Our Records Valuable?

- Jury Awards $20 Million in Damages for Value of Lost Records

Are Our Records at Risk?

- Are Our Records at Risk?
- Are Our Records at Risk?
- Are Our Records at Risk?

Bank Photo from Deanna Mello

- Bank Photo from Deanna Mello

Infopro (ARMA International)

- Infopro (ARMA International)

March/April, 2003

- March/April, 2003

Are Our Records at Risk?

- Are Our Records at Risk?

Courtesy of David B. Steward, CRM

- Courtesy of David B. Steward, CRM

Blackwell Sanders Peper Martin

- Blackwell Sanders Peper Martin

Are Our Records at Risk?

- Are Our Records at Risk?

- Are Our Records at Risk?
Vital Records Identification, Protection, and Disaster Recovery

June 16, 2009

Wess Jolley, CRM, Records Manager

Types of Disasters

- Natural disasters
  - Fires
  - Flood
  - Leaks
  - Structural
  - Hurricanes
  - Earthquakes
  - Infestations
  - Mildew
- Human disasters
  - Riots
  - Sabotage
  - Security Breach
  - Terrorism
  - Negligence
  - Carelessness
  - Accidents
  - Theft
  - Death of a vital employee

Minor or Severe

- The Most Minor
  - A lost file
  - Coffee spilled into a file drawer
  - A hard disk crash
  - An accidental discard
  - A broken pipe
- The Most Severe
  - Nuclear blast
  - Campus wide hurricane damage
  - Massive fire to a critical building
  - Destroyed buildings in an earthquake
  - Terrorist attack

Why Do We Bother to Plan?

- Three things to protect
  - People
  - Records
  - Equipment, Inventory, Everything Else

Consequences of Losing Vital Records

- In 1989, 630 businesses were affected by the Santa Cruz, California, earthquake. 15% never reopened.
- In 1993, 250 businesses were affected by floods in Chesterfield, Missouri. Only 52 reopened.
- 40% of companies that lose their records by fire fail to survive the next business year.

The Information Disaster Plan

- Part of your Departmental Records Management Manual
- “An information disaster plan is a written, approved, implemented and periodically tested program to identify, protect, and reconstruct/salvage an organization’s vital and historical records, and to establish procedures for the immediate resumption of business operations in the event of a disaster.”

Five Steps to the Creation of an Information Disaster Plan

1. Assess and reduce the risk of disasters
2. Identify the vital records
3. Protect the vital records
4. Ensure the ability to resume operations and reconstruct vital records in the event of a disaster
5. Document your disaster plan

Step 1

Assess and Reduce the Risks of Disaster
Conducting a Records Risk Analysis: Questions to Ask

- What are the possible threats to the records?
- What are the physical vulnerabilities from these threats?
- What are the vulnerabilities from human error or carelessness?
- Are there vulnerabilities in regard to building or equipment malfunction or failure?
- Is there a vulnerability to acts of deliberate destructiveness?

Records Risk Assessment Site Survey

- The geographical location of the facility or facilities
- The location of all records and information
- The media, enclosures, housing and storage environments of the records
- Existing potential hazards to records and information
- Any specific areas of vulnerability
- Existing alternative protection for vulnerable records and information

Records and Information Risk Assessment Site Survey

- Site Survey
  - The geographical location of the facility or facilities
  - The location of all records and information
  - The media, enclosures, housing and storage environments of the records
  - Existing potential hazards to records and information
  - Any specific areas of vulnerability
  - Existing alternative protection for vulnerable records and information

Risk Evaluation Equation

\[ P \times C = R \]

- \( P \) = Probability that a loss will be sustained in any given year (based on historical and other data)
- \( C \) = Cost of the loss (usually to replace the information in the records)
- \( R \) = Risk, or “Annualized Loss Expectancy”

An example

- The cost of replacing (or the consequences of the loss of) an important record set is estimated at $500,000.
- The probability of loss is 2% per year, or .02. In other words, the loss can be expected to occur an average of once every 50 years.
- The risk is calculated as $10,000 per year.
- Conclusion: This record set is worth protecting if it costs less than $10,000 per year to do so.

Take a Break!

- Be back in ten minutes...
Step 2
Identify the Vital Records

What is a “Vital Record”? *
- Two Criteria:
  - Any record which is required to re-establish critical functions in the event of an emergency
  - Records which are necessary to protect the legal and financial status of the College

Identifying the Vital Records
- The Records Inventory
- Obtain Departmental and Institutional Support
- Work Collaboratively
- Work Systematically
- Document your process!

Questions to Ask during the Inventory
- What records are absolutely necessary to resume critical functions?
- What would be the consequences of the absence of a record?
- What records are necessary to preserve the rights and obligations of students, employees, alumni, trustees, and the general public?
- Which records are unique and/or irreplaceable?

Questions to Ask, Cont.
- Which records are necessary in the short term?
- Which records are mission-critical?
- Are there other sources from which the records, or information on the records, can be retrieved?
  - Inside the College
  - Outside the College
- Do the records reside on more than one media?
- What about digital records????

Records Classification
(see handout)

**Vital Records**
- Records containing information critical to the continuation or survival of an organization during or immediately following a crisis
- They contain information necessary to continue operations without delay under unusual conditions
- They contain information necessary to recreate an organization’s legal and financial status and to preserve the rights and obligations of employees, customers, stockholders and citizens

**Important Records**
- Records and information on a variety of media determined to be of some value to the College in restoring operations to a normal state following a disaster
- If destroyed, these records can be replaced or recreated at moderate cost, in an acceptable time frame
Useful Records
- Records that are useful, but not essential, to the uninterrupted operation of the College.
- These records are replaceable in an acceptable time frame, or their loss would cause only temporary or acceptable inconvenience.
- Non-Records

Setting Recovery Priorities
- **VA**: Immediate Recovery, 1st Priority
  - Records and information essential for emergency operations
- **VB**: Immediate Recovery, 2nd Priority
  - Records and information essential for immediate resumption and continuation of business following a disaster
- **VC**: Immediate Recovery, 3rd Priority
  - Records and information essential for legal or audit purposes

Complete Classification and Recovery Priority Scheme
(five possible classifications):
- **VA**: Vital Records, 1st Recovery Priority
  - Records and information necessary for emergency operations
- **VB**: Vital Records, 2nd Recovery Priority
  - Records and information essential for immediate resumption and continuation of business following a disaster
- **VC**: Vital Records, 3rd Recovery Priority
  - Records and information essential for legal or audit purposes
- **IM**: Important Records
- **US**: Useful Records (and non-Records)

Typical Breakdown
- Important: 60%
- Vital: 5%
- Useful: 35%

General Protection Concept
- Record duplicates, stored in secure, off-site location(s)
- Reminder: We are talking about a SMALL percentage of your records!
- Probably no more than 3-10%
- Should be small, or the program will be too cumbersome to manage

Physical Records: Dispersal
- **Routine Dispersal**
  - Part of a routine business process
  - Not necessarily designed for vital records protection
  - Records maintained in two or more locations
  - Possibly on two or more different media
  - Records must be kept current, and be accessible when needed
  - Usually low or no cost
- **Designed Dispersal**
  - Specifically designed to protect vital records
  - A more costly option

Physical Records: Dispersal
- **Dispersal technology**
  - Photocopying
  - Imaging
  - Microfilming
  - Multi-part NCR forms

Physical Records: Protective Storage
- **Technologies**
  - Fire-resistant safes and vaults
  - Environmental control systems
  - Water shielding
- **Some protection, but ultimately unreliable**
Electronic Records: Data Backup

- Elements of a successful backup strategy
  - Regular
    - How much data can you afford to lose?
    - Daily?
  - Off-site
  - Duplicative
    - Short retention: disaster recovery only!
- Protection of vital electronic records is arguably more important than paper records, since media can fail without visible signs

Electronic Records: Other Protection Strategies

- Data Vaulting
- Data Replication
  - Transaction Aware Replication
  - Mirroring
  - Shadowing

Pitfall of Record Duplication: Meeting Retention Schedules

- How do you implement retention schedules for material that is dispersed through duplication?
- Utilize RM as your off-site location?
- A documented plan must be in place to handle retention and disposition!

Step 4
Ensure the Ability to Resume Operations and Reconstruct Vital Records

The Disaster Recovery Kit (see handout)

The Disaster Recovery Kit (see handout)

The Vital Records Schedule (see handout)

Based upon draft ANSI/ARMA Standard “Establishing a Vital Records Program”

Step 5
Document Your Disaster Plan

The Disaster Recovery Kit (see handout)

The Disaster Recovery Kit (see handout)
Disaster Plan Contents
- Vital Records Schedule
- Circumstances which activate the plan
- Response procedures
- Responsibility checklists
- Restoration procedures
- Contents of the disaster kit
- Vendor Contacts (freezing and recovery facilities)
- Sources for other supplies
- Complete phone contact information

Disaster Plan Maintenance
- New record series
- New operating locations
- Major modifications to existing space
- Change of address of disaster team
- Change of vendors
- Freshening supplies in the disaster kit

Test Your Plan!
- Full dry run
- Periodic
- Participation of all players
- Perform post-dry run review
- Update the plan as necessary
- Be sure to keep up to date on contents of the disaster kit, and contact phone numbers

When a Disaster Strikes
- Activate the plan
- Contact the Records Manager
- Prioritize your response:
  - Vital records first?
  - Perhaps not, if they are protected!
- Consider outside help

Salvage of Water-Damaged Records
(see handout)
- Paper
  - Dry within 48 hours
  - Otherwise, freeze
- Floppy disks, digital media, sound and video recordings
  - Seek professional help
- Photographs
  - Dry
  - Freeze
  - Rewash and dry

Drying Techniques
(see handout)
- Air Drying
- Dehumidification
- Freezer Drying
- Vacuum Thermal Drying
- Vacuum Freeze Drying

Utilizing Professional Services
BMS Catastrophe:
http://www.bmscat.com
http://www.muntersamerica.com

Mold Damage
BEFORE
AFTER
Vital Records Identification, Protection, and Disaster Recovery

Links of Interest
- ARMA
  - http://www.arma.org
- NARA
- State of Oregon
- University of Washington
  - http://www.washington.edu/admin/recmgmt/vital.records2.html
- “A Tale of Three Technologies”

PDF Forms
http://www.dartmouth.edu/~library/recmgmt/forms.html

What We Have Learned...
- We have defined a “Record”
- We have examined the components of a comprehensive Disaster Plan
  1. Assess and reduce the risk of disasters
  2. Identify the vital records
  3. Protect the vital records
  4. Ensure the ability to resume operations and reconstruct vital records in the event of a disaster
  5. Document your disaster plan

Questions and Discussion