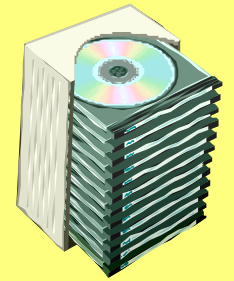


DIGITAL
IMAGING
to
EMPLOY PEOPLE
with
DEVELOPMENTAL
DISABILITIES



The Law

M.S. 15.17 M.S. 138.17

Please visit – <http://www.revisor.leg.state.mn.us/stats/15/17.html>
to read the complete statute:

Official records must be kept.

Responsibility for records.

Delivery to successor

Accessible to public

and

<http://www.revisor.leg.state.mn.us/stats/138/17.html>

Government records; administration.

Destruction, preservation, reproduction of records; prima facie evidence.

Records inspection

Transfer process

Access to archives records

Archivist; equipment; supplies

Records management program

Emergency records preservation

Optical disk standards

Optical image storage

STANDARDS

IRM Standard 12. Version 1:

Technical Standards for the Reproduction of Government Records Using Imaging Systems

The purpose of these standards is to establish technical archival requirements for imaging systems so that documents stored in such systems are available for retrieval for as long as any law requires. Technical requirements include, but are not limited to, storage media, scanning quality, image file headers, and compression techniques. Technical requirements do not include management, documentation, quality assurance, security procedures or storage facility requirements.

IRM Standard 12, Version 1: Technical Standards for the Reproduction of Government Records Using Imaging Systems

Issued: February 15, 1995

Effective Date: February 15, 1995

Supersedes: N/A

Applicability:

Who cares about these standards?

All Minnesota "public officers", as defined in Minnesota Statute 15.17, Subd 1.
<http://www.revisor.leg.state.mn.us/stats/15/17.html> (Affects all levels of Minnesota government)

When do they apply? When do they not apply?

These standards are mandatory when records are deemed to be permanent or archival. These standards represent the best practices identified by the industry for imaging systems. Therefore, in addition to the mandatory imaging requirements for permanent records, these standards are recommended for use with all imaging systems.

These standards do not prohibit the use of non-erasable optical imaging systems for the presentation of archival records without the preservation of paper or microfilm copies.

How Do I Know If The Records Are Permanent or Archival?

Records can be identified as permanent or archival in several ways.

- They are specifically required to be kept permanently by state statute.
- The public office responsible for the records designates them as permanent.
- They are designated as permanent by the state records disposition panel or identified as archival by the state archives as part of the process for submitting a request to dispose of original records. By statute, virtually no government record in Minnesota may be destroyed without prior authorization of the panel. Securing approval is a simple, one-time process that is described in a leaflet entitled Procedures for the Proper Disposal of Government Records which is available from the State Archives Department of the Minnesota Historical Society. The Archives staff provides assistance with this process. Determining the appropriate retention period of the source documents and securing the state records disposition panel's approval of the retention period selected should be completed before an imaging system becomes operational.

Purpose of Standards:

The purpose of these standards is to establish technical archival requirements for imaging systems so that documents stored in such systems are available for retrieval for as long as any law requires. Technical requirements include, but are not limited to, storage media, scanning quality, image file headers, and compression techniques. Technical requirements do not include management, documentation, quality assurance, security procedures or storage facility requirements (see "Management Standards for the Reproduction of Government Records Using Imaging Systems" also.)

Standard Requirements: Storage media:

- a) Only non-reusable media shall be used for imaging systems.
- b) The storage media used shall have a certified pre-write shelf life of at least five years and post-write shelf life of at least 20 years, based on accelerated aging tests that apply to specific locations on the media surface.

Scanner quality:

- b) Scanner quality must be evaluated based on the standard procedures in American National Standard for Information and Image Management - - Recommended Practices for Quality Control of Image Scanners. b) For textual documents: Scanning density no less than 200 dots per inch, type no smaller than 6 points. c) For engineering drawings, maps, documents with background detail or small type: Scanning density no less than 300 dots per inch. d) Scanners shall receive periodic maintenance as specified by the manufacturer and shall be recalibrated at least annually.

Image File Headers:

Standard (non-proprietary) image file header should be used. Since even some standard headers such as Tagged Image File Format (TIFF) are available in a variety of implementations, the vendor should supply a detailed definition of the image file header structure employed. If a proprietary header is used, the system must provide a bridge to a non-proprietary header label standard such as ANSI/AIIM MS53, File Format for Storage and Exchange of Images, or Bi-level File Format: Part 1.

PROTECTING THE DATA RECEIVED FROM A GOVERNMENT ENTITY

Government entities will have two concerns: (1) original documents where there are no copies and (2) documents that contain data that are not public. In both cases, a vendor will need a way to keep the documents secure.

Security may include the physical security of the documents as well as not disclosing their content. If a government entity has not indicated the security requirements for the documents in the request for proposal, ask for them.

For more information on how data in documents are classified, see “laws that classify data”. There are additional resources available in a companion document that may be of assistance.

Some government entities develop policies and procedures that tell their employees how documents and data are to be handled. Ask the government entity if it has this kind of policy and review it if one exists.

What follows is an example of this type of policy and procedure. It was developed by the Minnesota Department of Health and is used as part of a comprehensive program to help employees meet their legal responsibilities to protect the data held by the Department.

MDH

DATA PRACTICES

MINNESOTA DEPARTMENT OF HEALTH EMPLOYEE DATA PRACTICES AND DATA SECURITY CHECKLIST

This checklist is to inform you, as an employee of the Minnesota Department of Health (MDH), of the responsibilities you have regarding both data practices and data security. Your responsibilities regarding both data practices and data security are extremely important in performing your job as an employee of MDH.

SECTION I: DATA PRACTICES

The Minnesota Government Data Practices Act (Minnesota Statutes, chapter 13) governs how the Minnesota Department of Health (MDH) collects, receives, or maintains data. The Minnesota Government Data Practices Act requires MDH to:

1. Safeguard the privacy rights of data subjects; and
2. Facilitate access to all government data that should be rightfully disclosed

All MDH data are "public" unless otherwise classified by statute or temporary classification. Data may be classified as "private" or "nonpublic" (data are accessible only to the subject of the data and certain other persons or entities authorized by law), or data may be classified as "confidential" or "protected nonpublic" (data are not accessible to the subject of the data). All data that are not "public" data will hereafter be called "not public" data.

UNDERSTANDING OF DATA PRACTICES RESPONSIBILITIES

As an MDH employee, I acknowledge my responsibilities in dealing with data as follows:

A. DATA RESPONSIBILITIES

- will protect "not public" data on individuals or organizations that I collect, receive, or maintain in performing the duties of my position.
- will protect "not public" data I access through computer-related media or other media such as paper files, faxes, written reports, and verbal reports.

B. CONTACT SUPERVISOR

- When I have any doubts as to the classification, access, or release of data, I will contact my supervisor as soon as possible.

C. ACCESS TO "NOT PUBLIC" DATA

- I will protect "not public" data and release them outside MDH only to those authorized by law to receive them.
- I will share "not public" data with MDH staff only if they need them for their job.
- I will contact my supervisor if I have any questions about the release of "not public" data.
- If I receive any requests for personnel data, or any questions about the release" of personnel data, I will direct the requests and questions to the MDH Human Resources Office.

D. ACCESS TO PUBLIC DATA

- I will make public data available to persons appropriately.
- I will contact my supervisor if I have questions regarding any public data and how I should handle them.

E. MAINTAIN DOCUMENTS IN A SECURE MANNER

- I will physically maintain documents containing "not public" data in a manner that complies with security safeguards. Possible safeguards for documents that include "not public" data include: turning them face down or putting them away when visitors come to my desk or when I am away from my desk during the day, and storing them in a locked area overnight.
- If I do not have access to a locked area for "not public" data, I will contact my supervisor so that a locked area can be made available to me.
- I will not leave "not public" documents in public areas such as an open copy machine, fax machine, or printer.
- I will maintain electronic documents according to the guidelines set forth in Section II.

F. SAFEGUARDS FOR PROTECTING "NOT PUBLIC" DATA

- I will consult with my supervisor to learn about appropriate safeguards for the "not public" data with which I work.
- I will not share "not public" data with any unauthorized person while I am an employee at MDH and after I leave my employment at MDH.

G. DISPOSE OF DOCUMENTS IN A SECURE MANNER

- I will dispose of documents containing "not public" data in a manner that complies with security safeguards and MDH records retention schedules.
- When it is appropriate to discard paper documents, such as draft documents containing "not public" data, I will shred these documents.
- I will contact my supervisor about how to properly dispose of electronic documents.

H. THREAT OR UNAUTHORIZED ACCESS

- I will inform my supervisor immediately if I suspect a possible threat to, or the unauthorized access to, or release of "not public" data.

I. OPPORTUNITY TO ASK QUESTIONS

- I have had the opportunity to ask any questions about the data practices information above and I have had all of my questions answered.

SECTION II: DATA SECURITY

The following information is based on the MDH Information Resource Security Policy. It's goal is to inform you, as an MDH employee, of your responsibilities to maintain the security and integrity of agency information resources. Learning about your responsibilities and the tools available to you will facilitate your ability to protect the data you work with and comply with the Minnesota Data Practices Act and other laws, rules, and policies.

UNDERSTANDING OF DATA SECURITY RESPONSIBILITIES

As an MDH employee, I acknowledge my responsibilities in dealing with data security as follows:

A. FIGHTING VIRUSES

- I will contact my system administrator for training on the use of anti-virus software, as directed by my supervisor.
- I will check for viruses on email attachments, floppy disks, Internet downloads, etc., if the information received is not checked for viruses automatically. I will also either delete, or check for viruses on, email messages that look suspicious, uncommon, or out of the ordinary.
- I will alert my division IT staff immediately if I suspect that my workstation has been infected with a virus.

B. PROTECTING COMPUTER LOGIN ACCOUNTS

- I will choose a unique password that is a minimum of eight characters, that is not a dictionary word, and that has at least two non-alphabetic characters.
- I will take reasonable precautions to safeguard my computer account from unauthorized use.
- I will keep my password private (i.e., I will not share it with anyone unless authorized by my supervisor).
- I will keep any written passwords in a location that is not readily accessible.
- I will change my password immediately and notify my system administrator if my computer account appears compromised.
- I will enter my password each time I log in rather than saving my password (i.e., I will not click 'remember my password' in the login box).

C. LOADING SOFTWARE AND INSTALLING HARDWARE

- I will use only legal copies of copyrighted software that are approved by the program manager and network administrator.
- I will contact division IT staff if I want software and hardware installed and follow their instructions for installation.
- I understand that authorized software and hardware will be installed according to approved methods.

D. REMOTE ACCESS TO THE NETWORK

- I will obtain approval from my supervisor/manager for dial-in access.
- I will obtain approval from my assistant division director for Virtual Private Network (VPN) access.
- I will take reasonable precautions to ensure the security of remote dial-in computer systems/devices and prevent theft, loss, or damage.
- I will adhere to all MDH Information Resource Security Policy requirements while using remote access systems.

E. SECURING MY PHYSICAL ENVIRONMENT

- I will ensure that portable electronic devices (such as laptops, personal digital assistants like Palm Pilots, etc.) belonging to MDH are not left unattended in unsecured areas.
- If directed by my supervisor, I will use a filter for my computer screen, or position my workstation monitor so that unauthorized persons cannot readily look over my shoulder to read "not public" data.
- If necessary, I will activate and password protect the screen saver when leaving my work area with "not public" data on the screen. The password protected screensaver should have no greater than a fifteen-minute delay before activation.
- When leaving my computer workstation for hours at a time, I will logoff or activate my password protected screensaver. My program manager and system administrator may authorize not logging off for special purposes (such as running a job overnight).
- I will secure "not public" data while working at an off-site location.

F. ENCRYPTING DATA

- I will contact my system administrator if I need assistance with encrypting data.
- I will ensure that all "not public" data located on transportable media and equipment (such as laptop computers, personal digital assistants like Palm Pilots, floppy disks, Zip cassettes, etc.) are encrypted as required by the MDH Information Resource Security Policy
- I will not send any data classified as "not public" over either email or other Internet systems unless the data are appropriately encrypted, encoded, or protected as required by the *MDH/Information Resource Security Policy*.

G. USING E-MAIL AND THE INTERNET

- I will read and be familiar with the *MDH Internet/Email Usage Policy*.
- I will ensure that my use of email and the Internet for both work related and personal reasons is in accordance with the *MDH Internet/Email Usage Policy*.

H. KEEP INFORMED

- I will seek permission from my supervisor to attend departmental and network, information security classes.
- I will read and be familiar with *MDH Information Resource Security Policy*.

I acknowledge that I have been informed of and understand my responsibilities contained in this checklist, and I have had the opportunity to have my questions answered. I also acknowledge my responsibility to comply with the Data Practices Act. A willful violation of the act is a misdemeanor and could lead to discipline ranging from reprimand up to loss of job.

Employee Name: _____ Date: _____

Position: _____ Program: _____

Signature: _____

Check one of the following:

- I have explained the items contained in this checklist to this employee and I have provided answers to any questions, or
- I verify that this employee attended training that covered the items in this checklist.

Name: _____ Date: _____
(Supervisor or Manager)

Position: _____ Program: _____

Signature: _____

MDH Employee Acknowledgement of Data Practices and Security Responsibilities Checklist
Data Practices Coordinator: Dave Orren, (651) 282-6310
Last Edited: February 21, 2003


EVALUATING SCANNING STEPS

To evaluate how a document in a project might be scanned, look at the steps in scanner manuals. These manuals will give you some ideas on how a particular project could be managed.


Examples of scanner manuals can be found in the following ways.

1. Hewlett-Packard: go to www.hp.com
Choose "fax, copiers, scanners"
Scroll down to "scanners"
Choose "for business" in the left column
Choose a model of scanner
Look in the technical support box on the right for "product information"
Choose "manuals" and look at the steps that are listed
2. Kodak: go to <http://www.kodak.com/>
Click on the "Business and Government" tab
Choose "document imaging"
Choose "imaging products"
Select "document scanners"
Choose a model
Click on "user publications"
Click on "user guide"
3. Fujitsu: go to <http://www.fujitsu.com/>
Select "United States"
Choose "services and products"
Select "computing products"
Click on "scanners"
Choose a model
Select either "product manual" or "user guide"

SCANNING STEPS

TERMS: Folder = Paper Folder 

Document = Paper Document 

File = Electronic file on the computer— shows as an icon on the screen 

Directory = Electronic folder containing files— shows as a “folder” icon on the screen 

NOTE

To get the correct results
these steps **MUST** be followed
EVERY time a document is
scanned

Scan only 8.5 x 11 standard thickness pages (20# weight, text). (See job coach duties). If thinner or thicker pages are found, or colored paper has been used, make a copy of these pages before scanning.

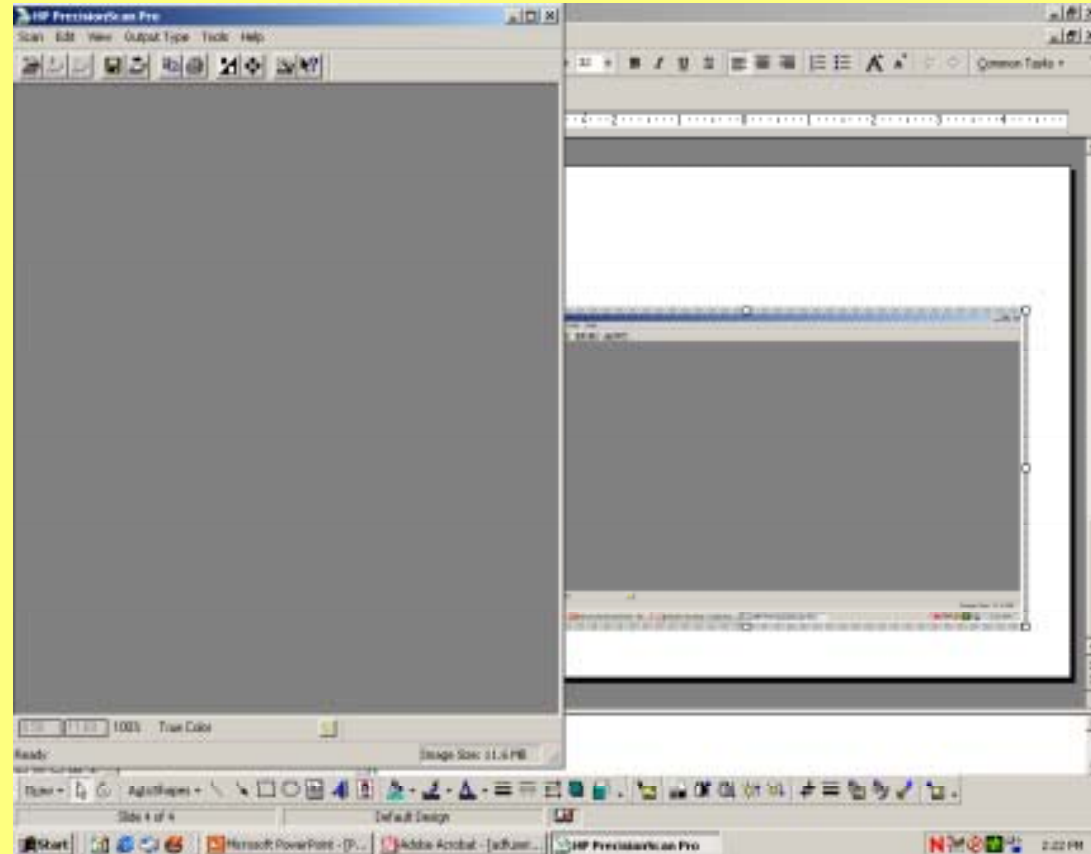
Legal size and newspaper clippings require specific settings; you will not be scanning these kinds of pages. Please notify the contact person if you find/have any of these types of documents at the end of each day.

Log onto the System
Press
Control Alt Delete
Type in your password
Press Enter

Double Click the scanner icon
on the desktop to start up
the scanner software

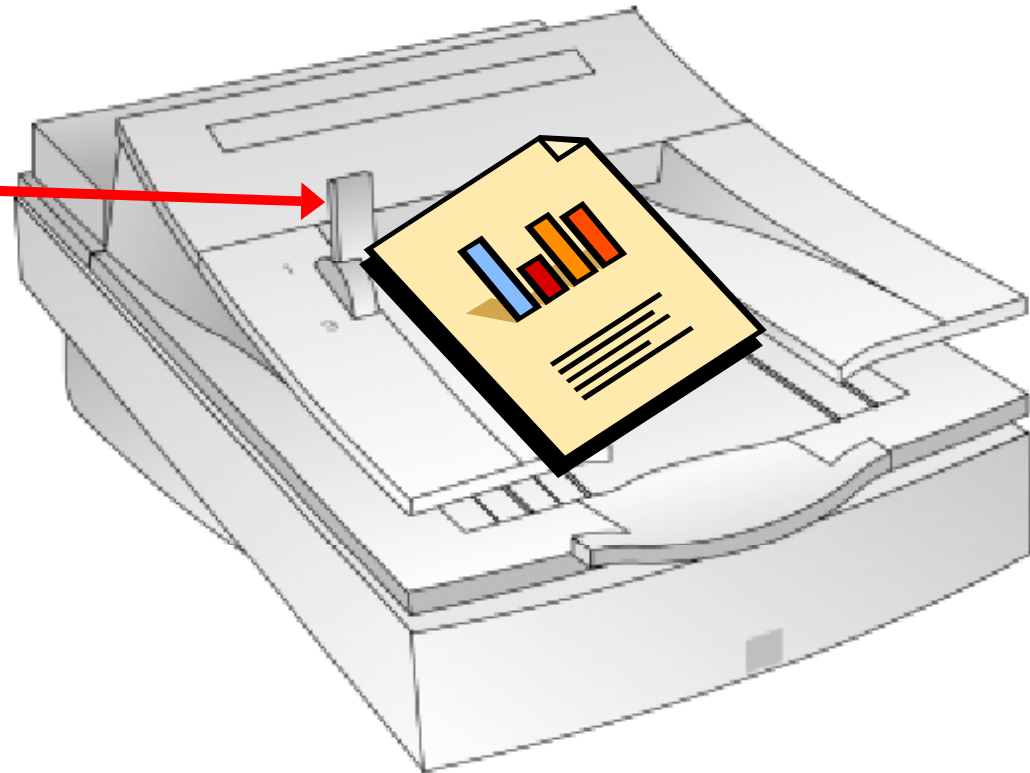


You should then see this window



Place a page of the document, in the scanner, face up, head first in the input tray. (Remember: keep all pages of the documents in order)

Make sure the paper load lever is in the #1 Position, push the page of the document up against the side of the ADF (or feeder tray) input tray nearest the lever. Move the paper load lever to the #3 position.

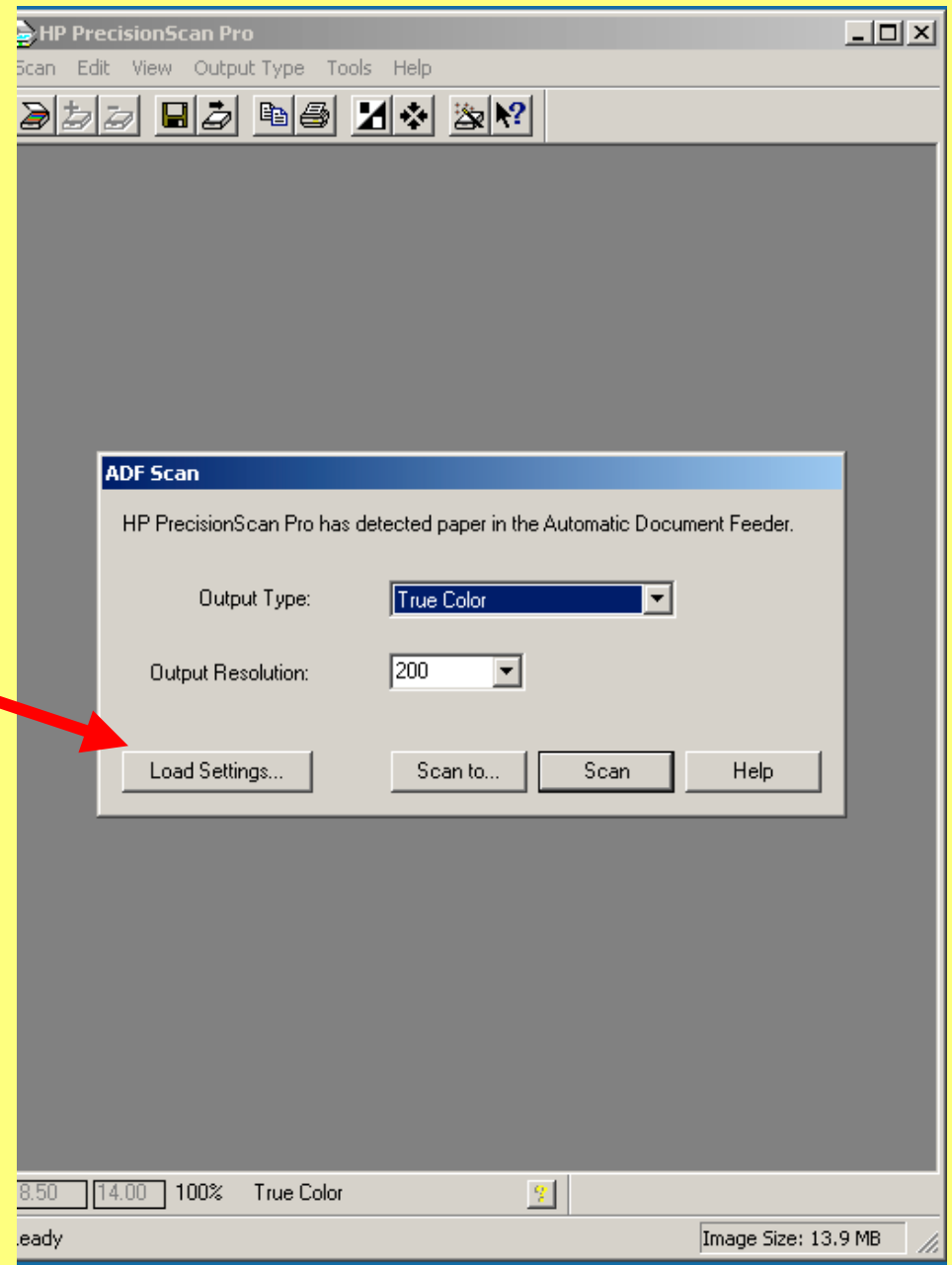


When you have clicked the paper load lever into the 3rd position you will then see . . .

This window.

Click on Load Settings

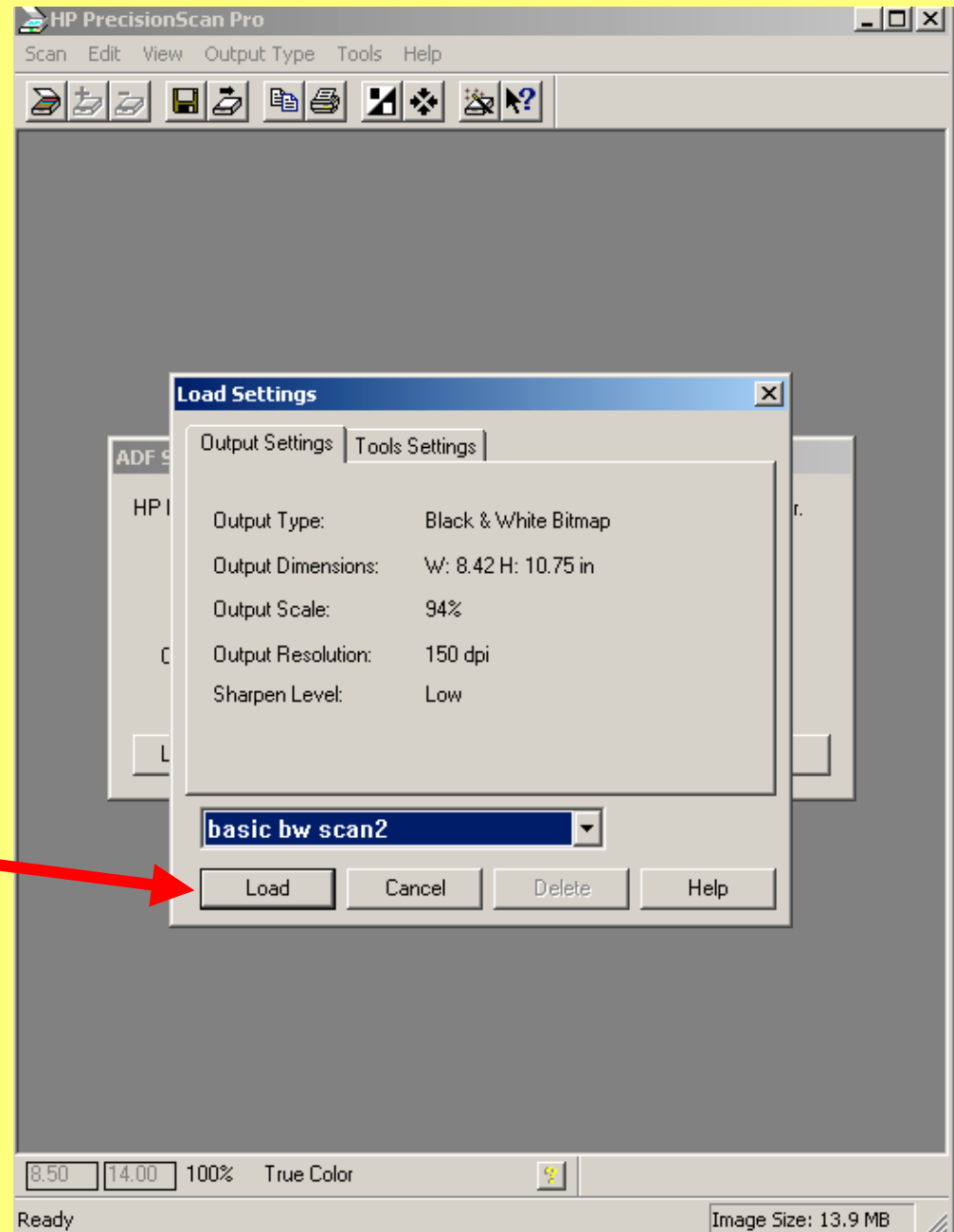
You will then see



This window.

Click on Load

You will then see . . .



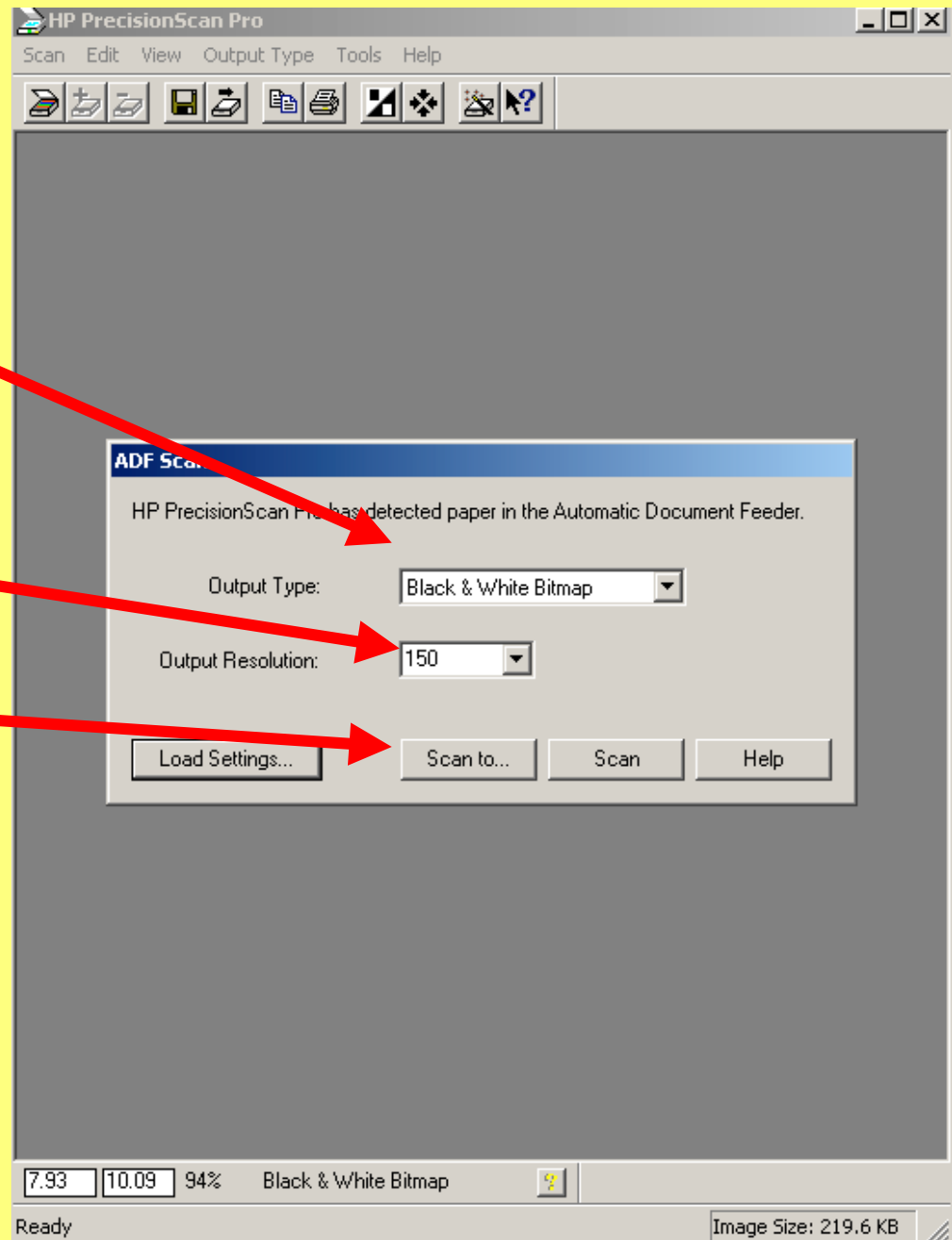
This window.

Make sure it is set for
Black & white bitmap

Output Resolution is
set at 150

Click on Scan to

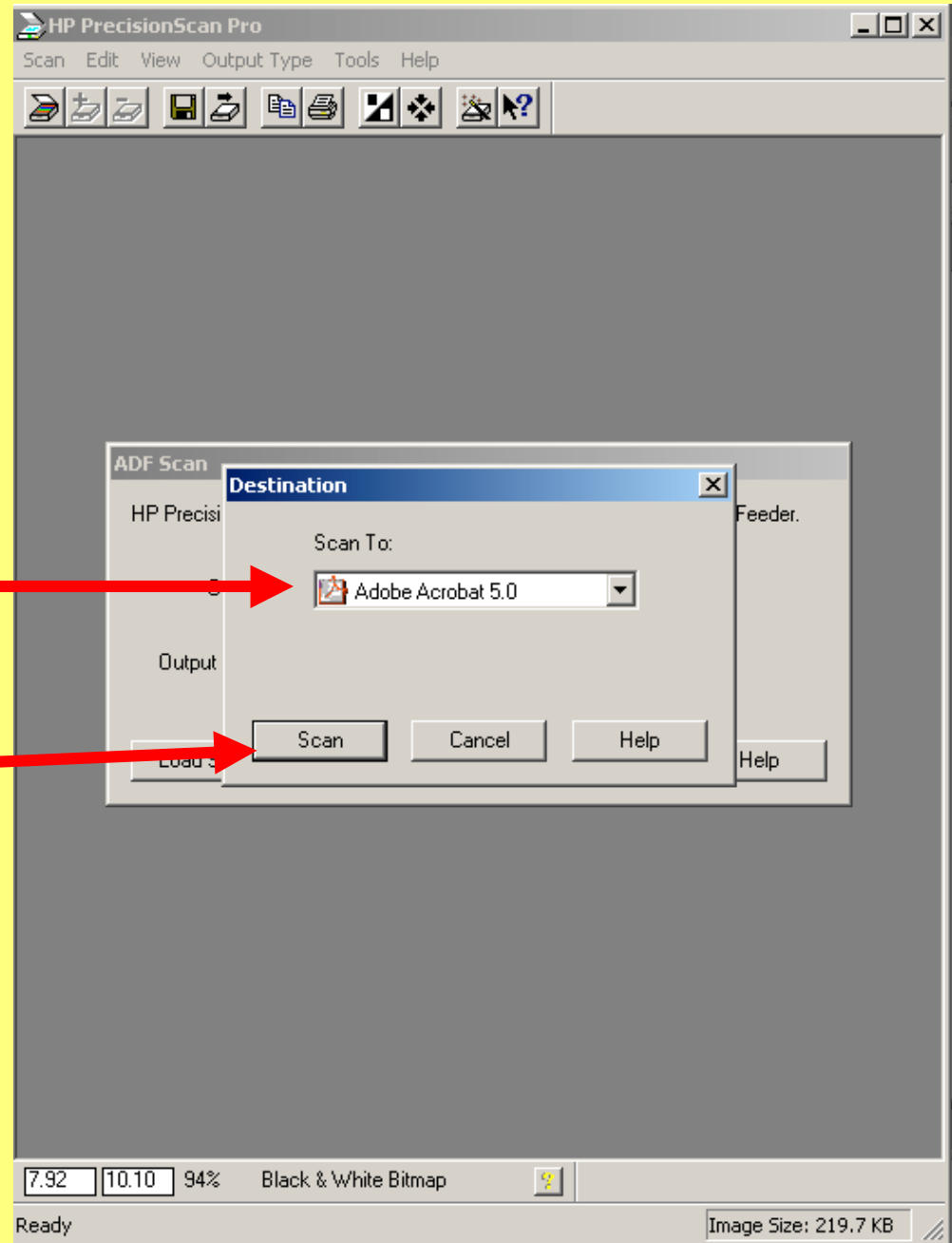
You will then see . . .



This window.

Make sure it is set to
Scan To:
Adobe Acrobat 5.0

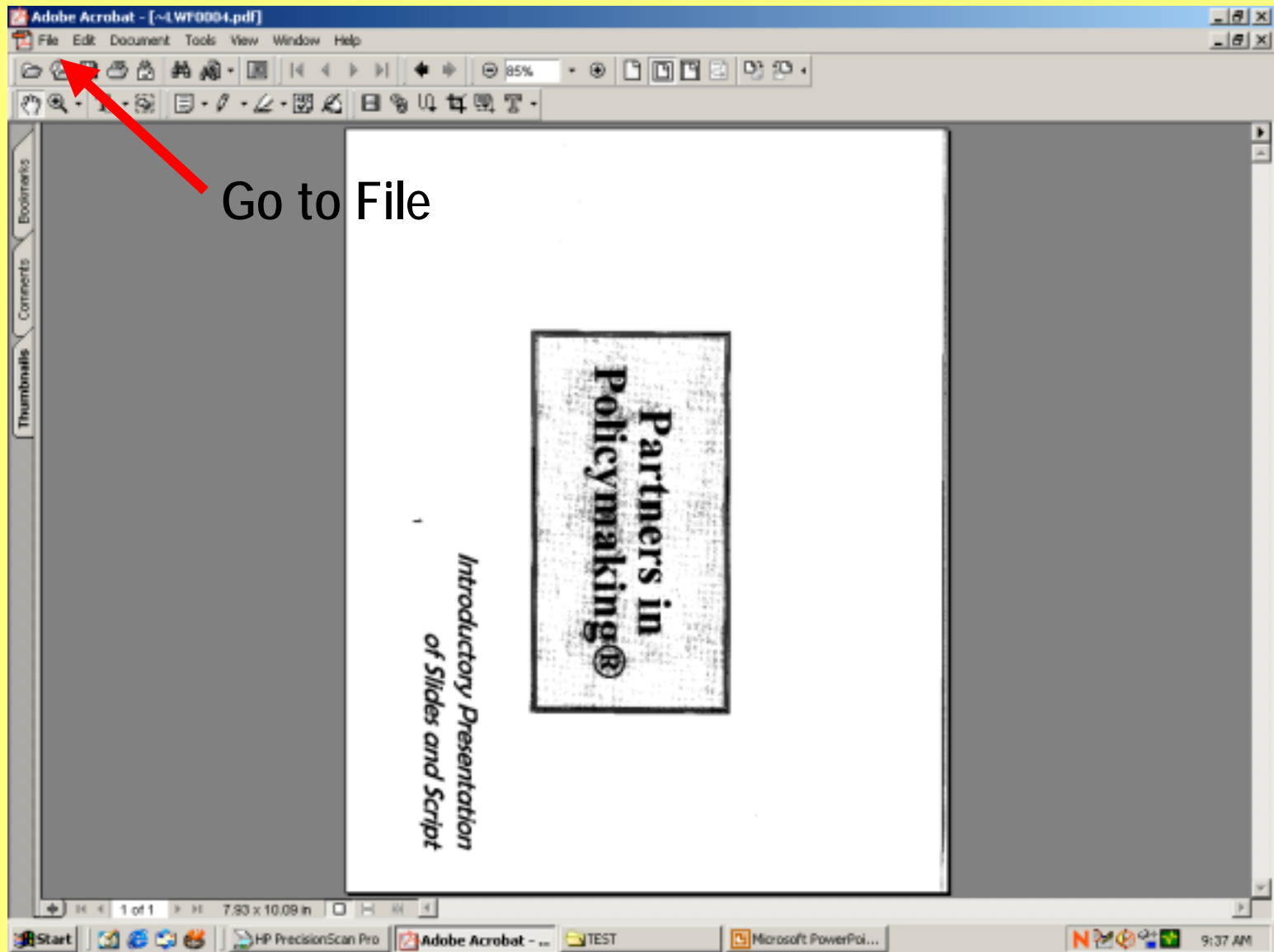
Click the Scan Button



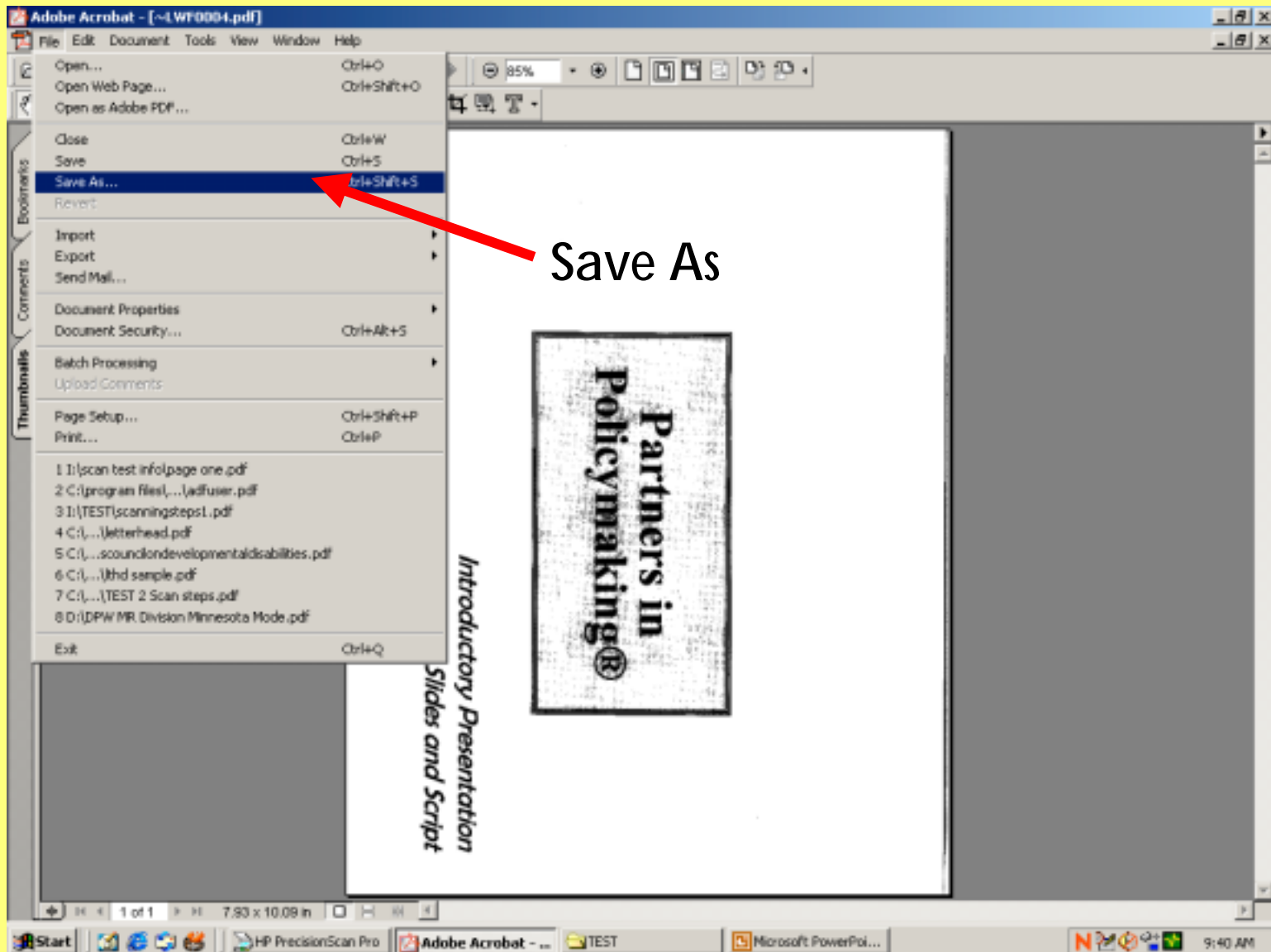
The scanner will then begin to scan the page of your document.

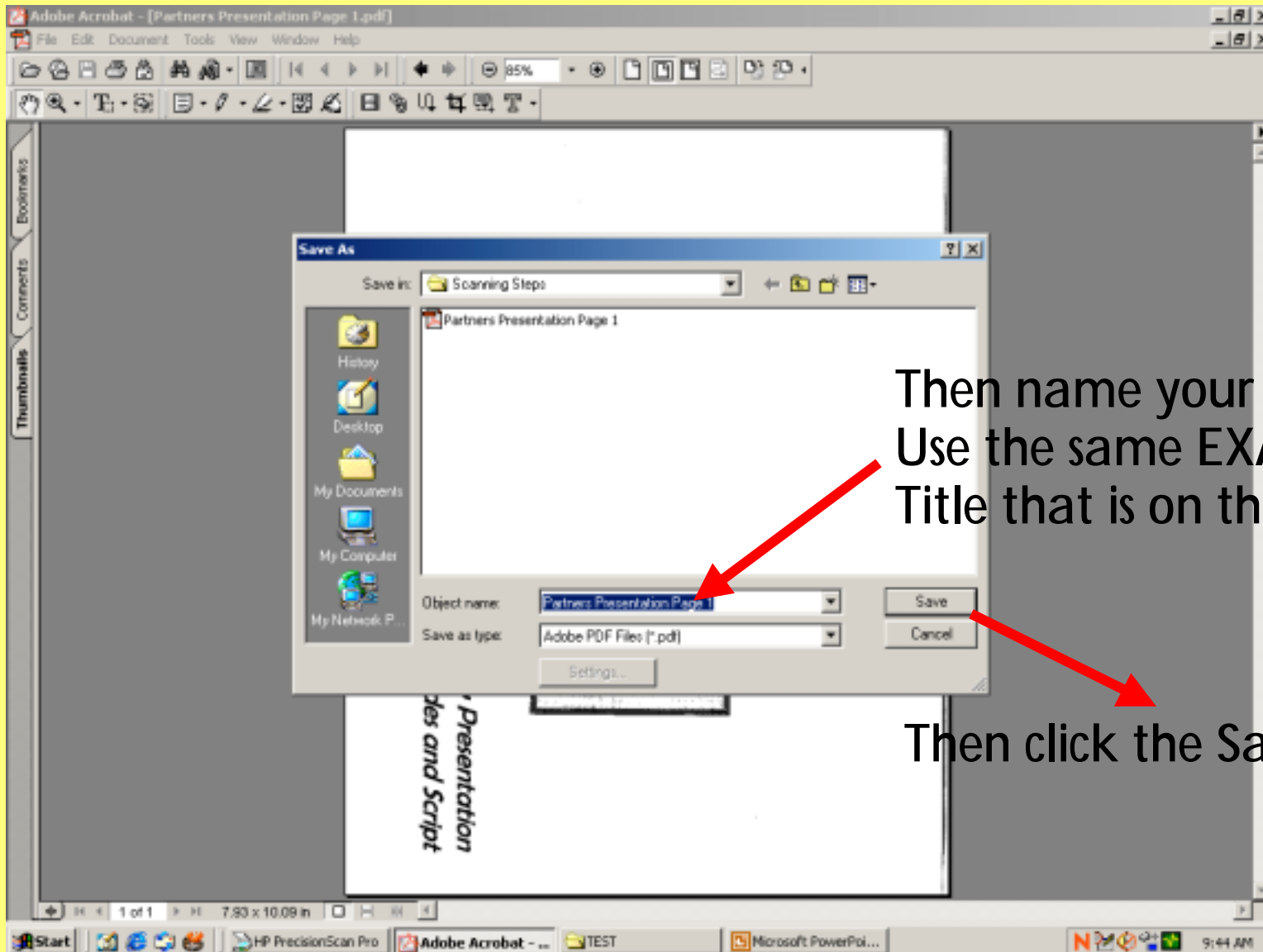
You will then see your scanned page in Adobe Acrobat (see next page).

You will then see a window like this



Go to File



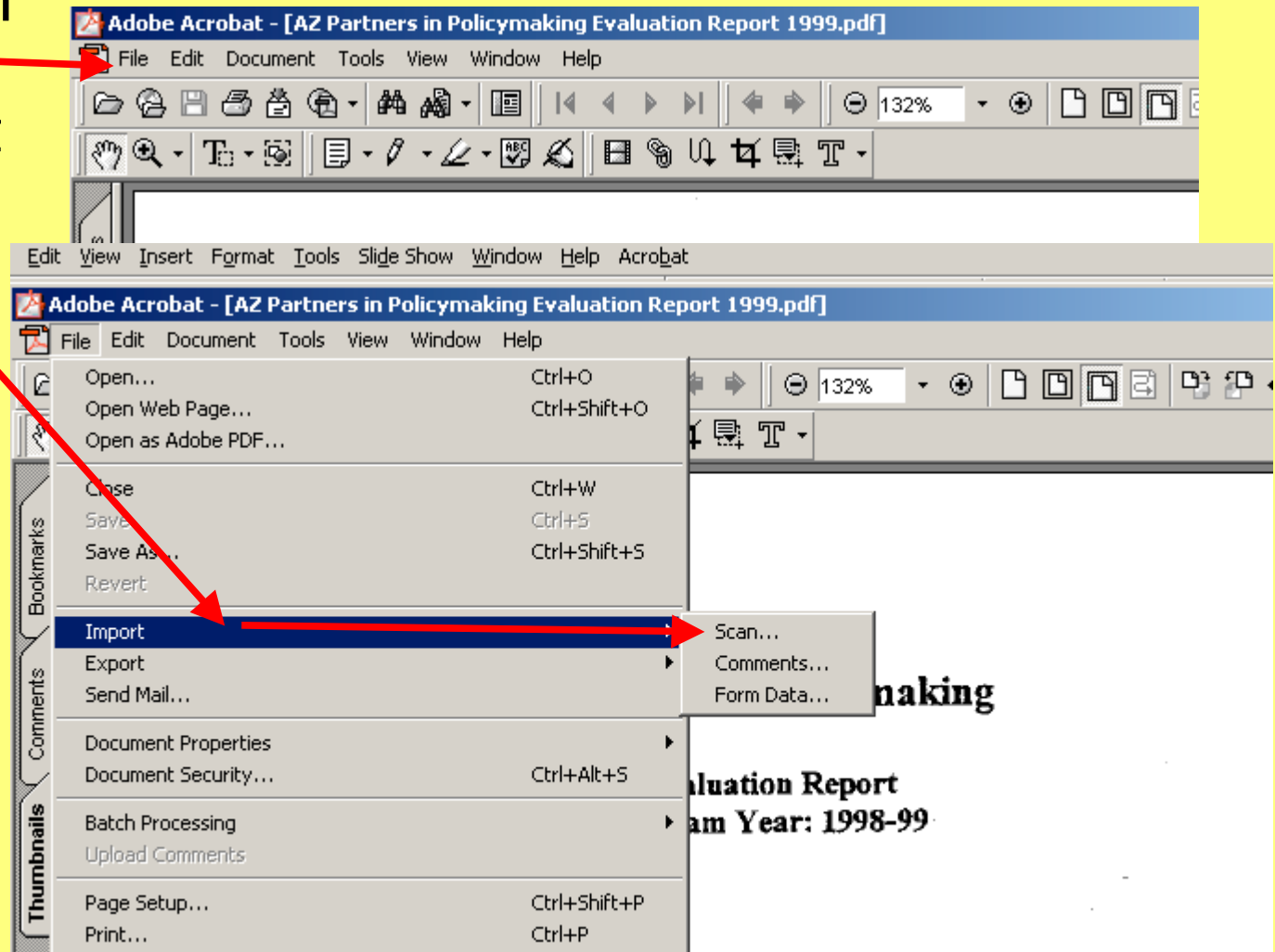


Then name your file -
Use the same EXACT
Title that is on the folder

Then click the Save button

Then get the next page of your document, and place it in the scanner, make sure the load lever is in the #3 position.

Then open your file go to file
Then to Import
and Scan

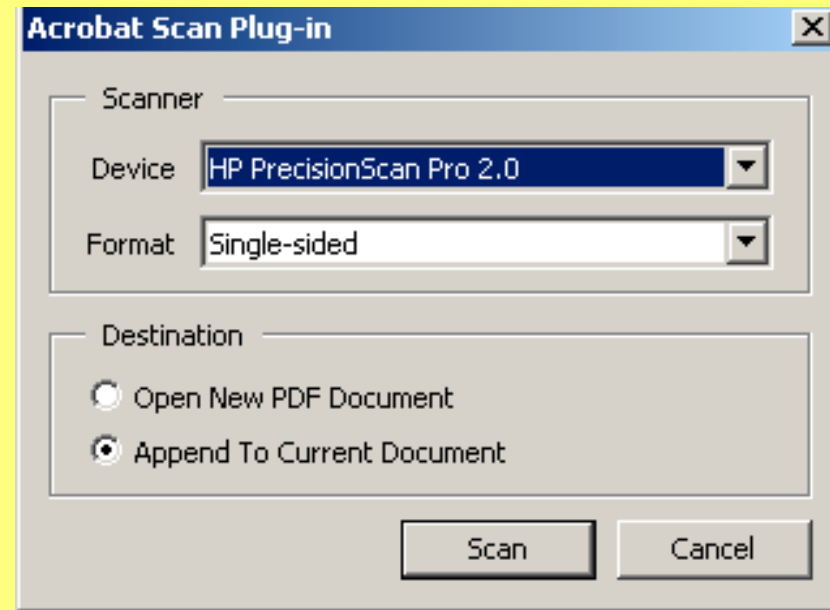


This window will then pop up
It should read as shown:

Device: HP Precision Scan Pro 2.0
Format: Single Sided
and
Append to Current Document
should be checked

Then click Scan

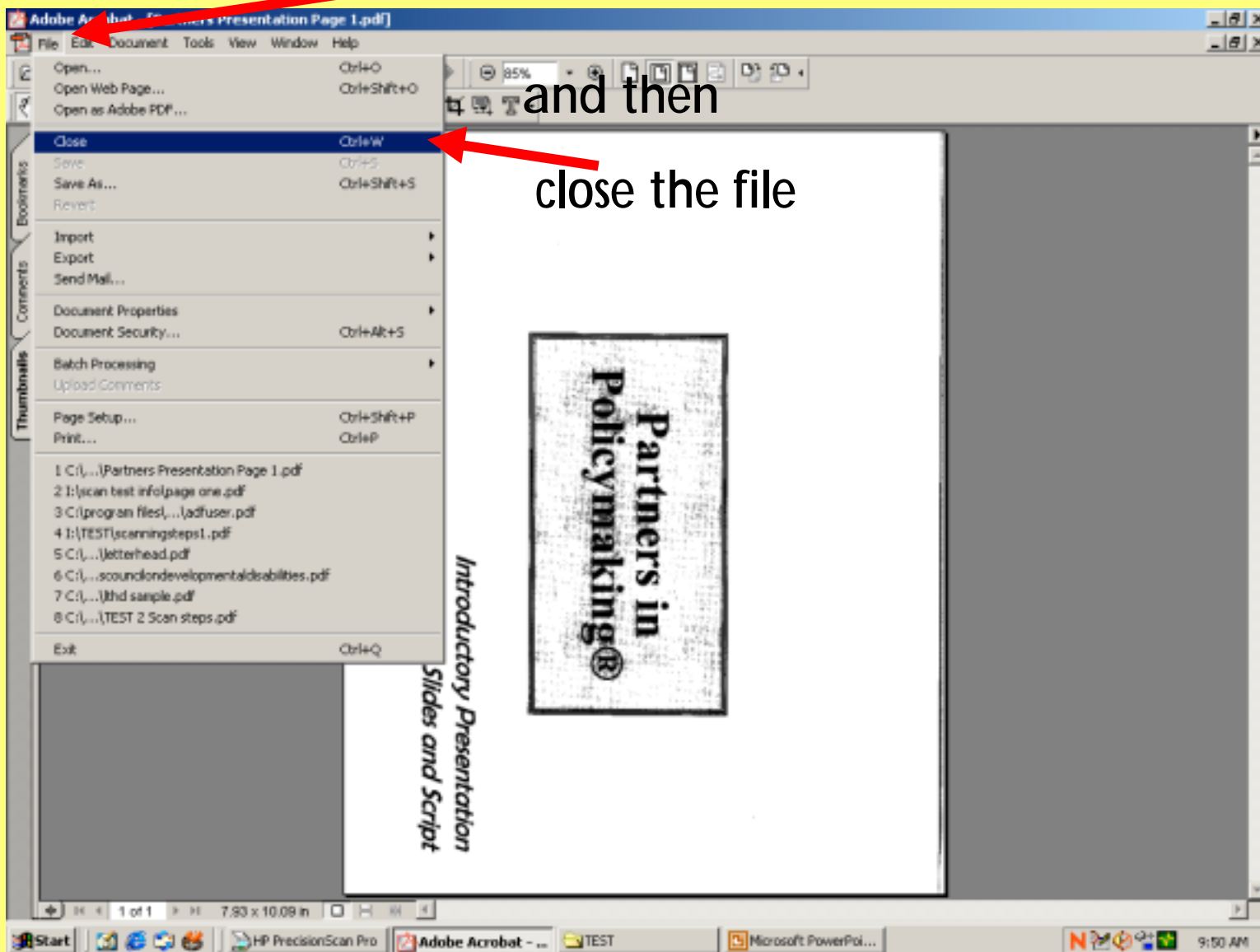
Follow the previous two pages until all documents
are scanned from the folder



Go to File

and then

close the file

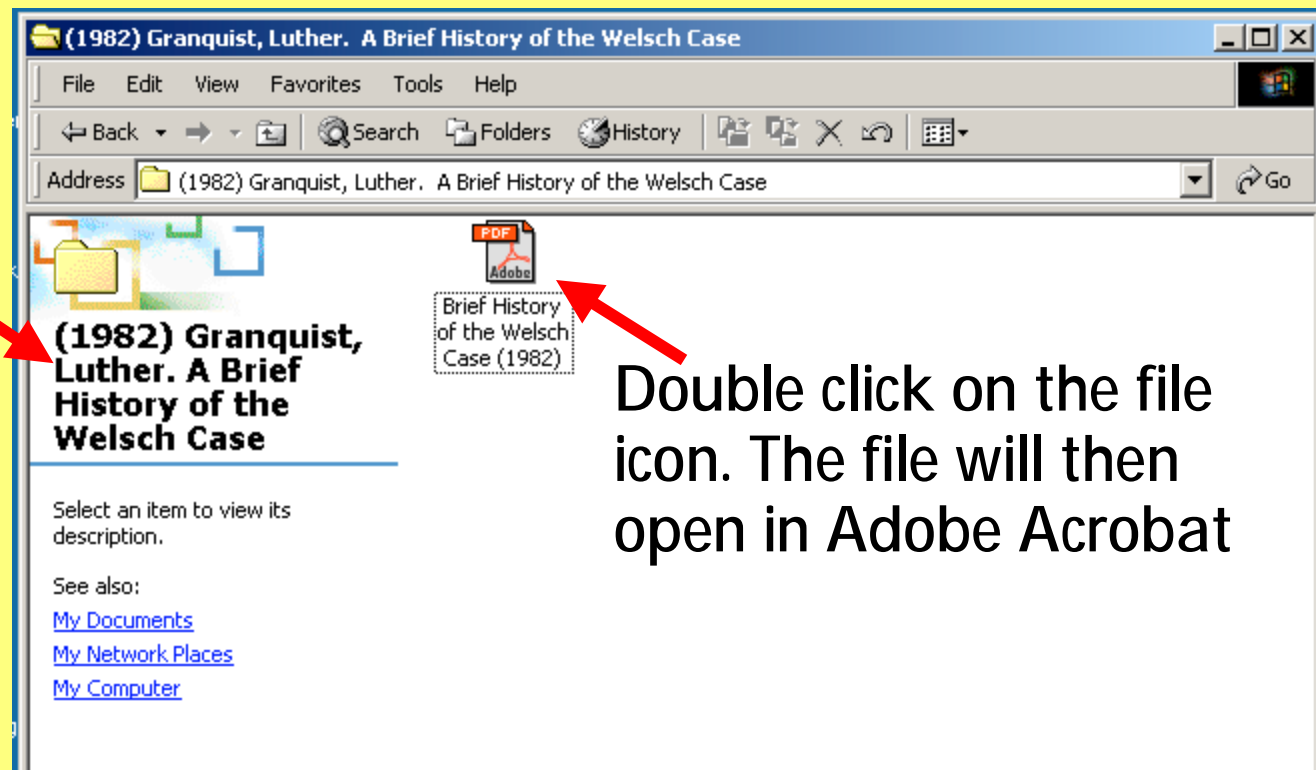


When all documents in your folder have been scanned open the file in Adobe Acrobat, click on "fit in window", so you can see the whole document, and check it to make sure it has been scanned properly:

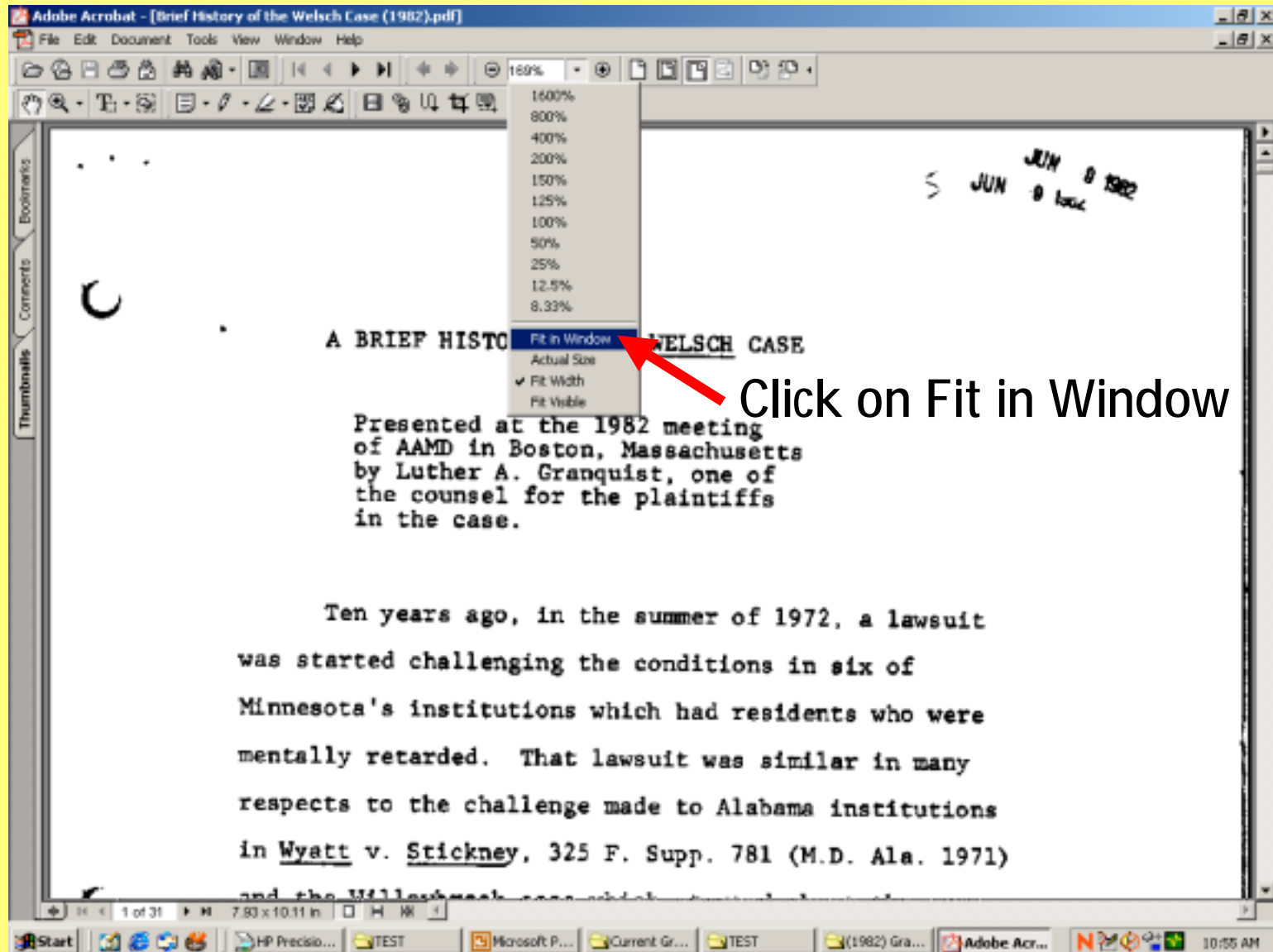
1. All pages should be readable;
2. Line up correctly

ie. type cannot be upside down, or cut off, all pages have to be there

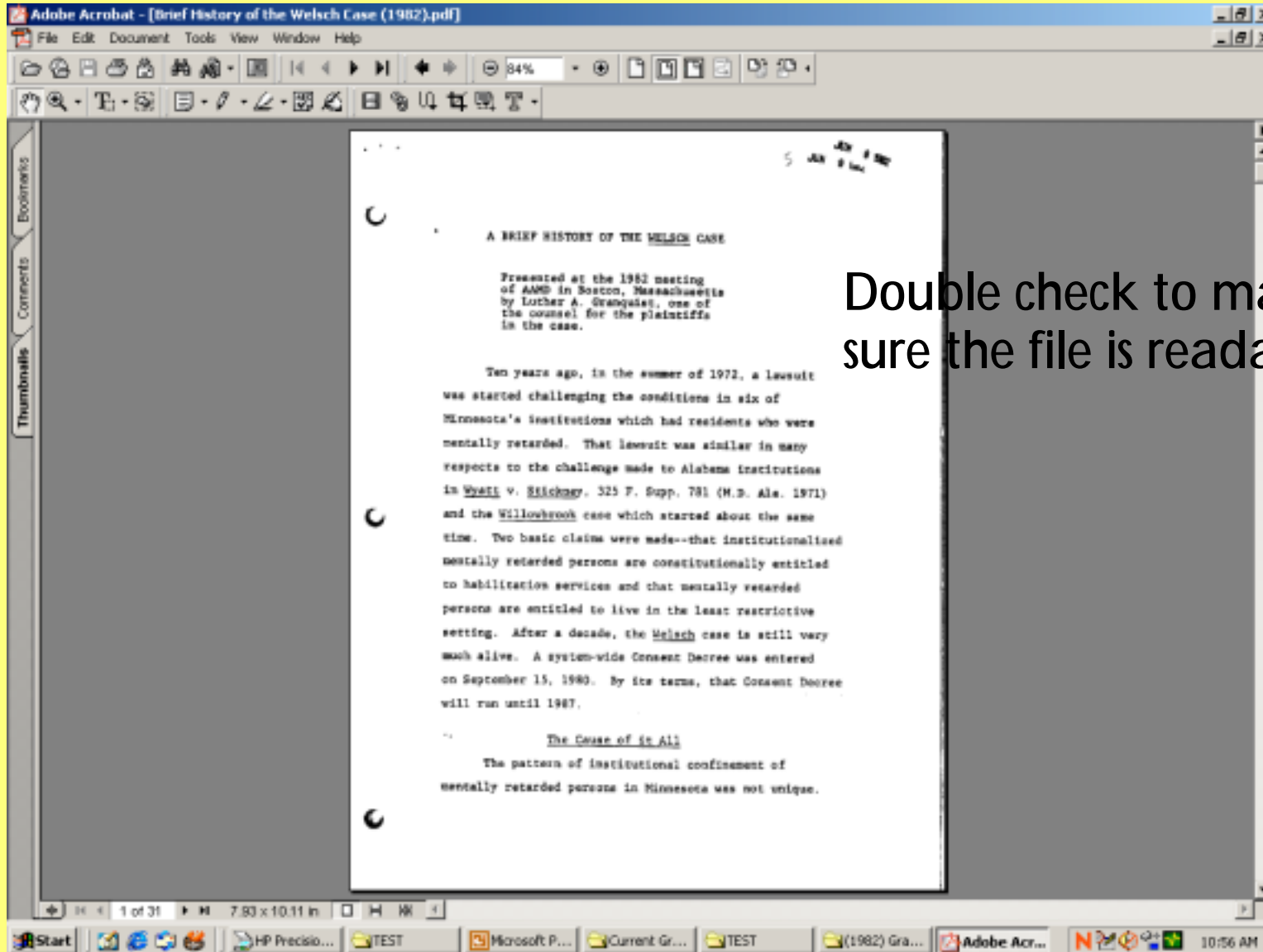
This is the name of the Directory you are in



Double click on the file icon. The file will then open in Adobe Acrobat



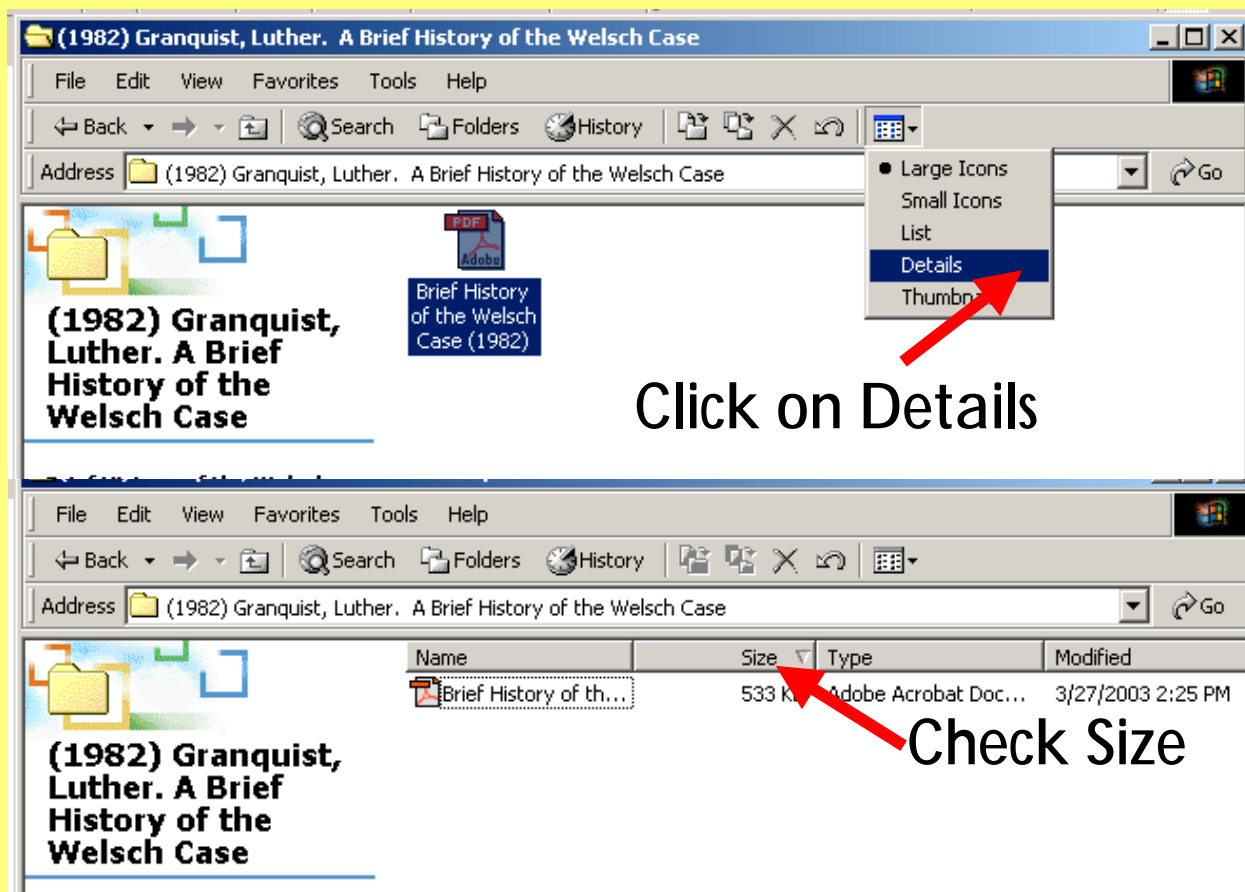
Click on Fit in Window



Double check to make sure the file is readable

Check the file size to make sure that the file has been scanned at the proper settings:

1. Locate your directory (folder icon), where the scanned files are saved in Windows.
2. Choose "details" from the "view" menu at the top;



3. File size appears in the "size" column. Most files will be less than 200kb. A very large document with a large number of pages might make a file more than 500kb.

If the file size is over 1 MB verify that the document has at least 40 pages. If the file has only a few pages it was scanned at an incorrect resolution Make sure that the “load settings” step is done when rescanning.

Do not delete the documents from the hard drive.

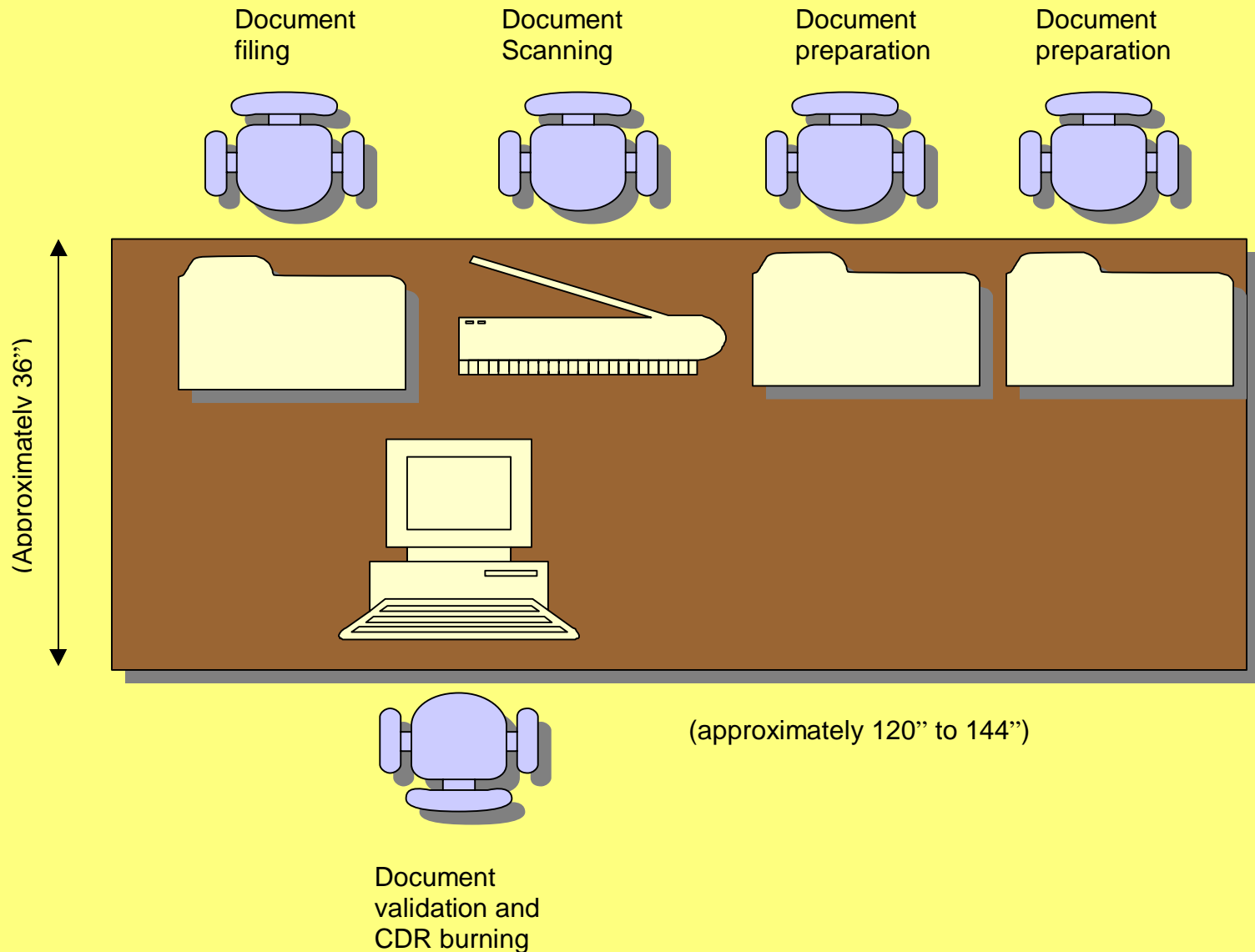
EQUIPMENT NEEDS

At a minimum, a vendor will need a personal computer (PC), scanner and printer to perform imaging work. Depending on the work to be performed and the government entity's requirements, the vendor may need a network or Internet connection.

There are at least two options for workstation layout when performing digital imaging. What follows are two options for workstation layout that may be of assistance as you plan how to accomplish the work.

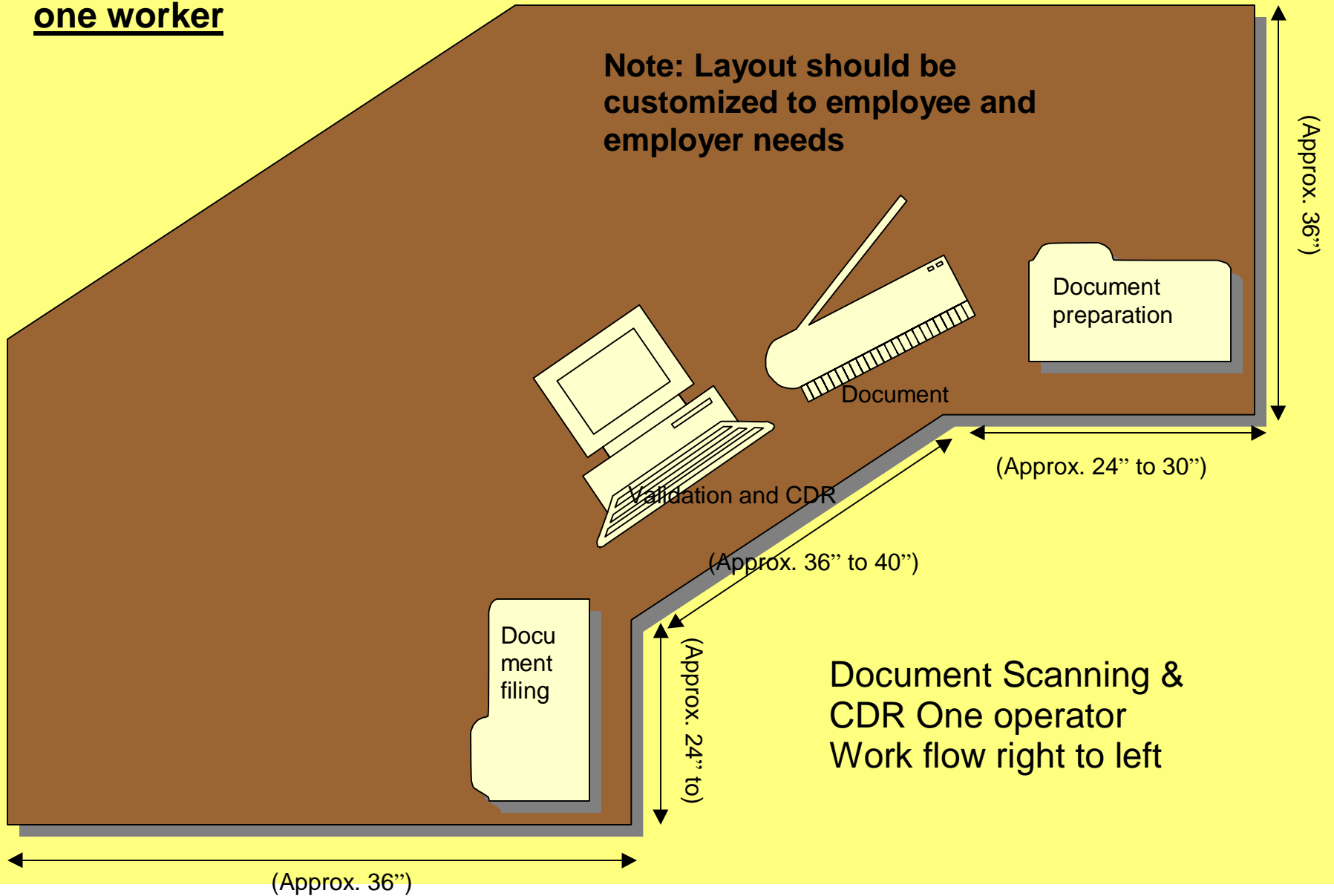
Document scanning 'team'

Note: Layout should be customized to employee and employer needs the options of number of workstations and physical layout depend on, skill of workers, worker accommodations, and employers needs. This example is a typical 5 person "team".



Document Scanning
one worker

Note: Layout should be customized to employee and employer needs



ADDITIONAL HELPFUL INFORMATION

As you consider digital imaging work, additional information may be of assistance. What follows are a scanning preparation checklist, information about job coaches and how to label the paper records.

The preparation checklist was developed as part of an imaging project. Each project will have unique requirements; this checklist should give you an idea of what might need to be accomplished to get the documents ready to be scanned. A government entity may detail the document preparation requirements as part of a request for proposal. If it is not clear what preparation a vendor will need to do, be sure to ask for that information.

A job coach assists employees with developmental disabilities with job duties and other tasks. The information that follows gives vendors an idea of what a job coach can be asked to do to assist employees and how they can help them be successful.

The labeling steps are included to help vendors plan what needs to be done with the documents once the scanning is complete. The request for proposal may or may not ask the vendor to perform these tasks. If the request for proposal is not clear, be sure to ask.

SCAN PREPARATION CHECKLIST

Folder = paper folder

Document = paper document

- Identify documents to be scanned
- Place document (or documents that need to stay together) in a folder
- Sort/organize folders according to:
 - Retain CD with scanned documents for internal use
 - Retain CD; folder to be transferred to MN Historical Society
 - CD with scanned document(s) for web site placement
- Review documents in each folder for completeness, place in order (chronological, other), remove items that don't need to be scanned
- Remove legal size pages, newspaper clippings, photos
- Mark (post-it) pages in each document "copy before scanning" for pages on colored paper, pages <> 20# text weight)
- Organize folders by fiscal year, major categories/headings, etc.
- Write document title on each folder: author (if known, relevant), name of document, year
- Place folders in box
- Create dividers; note category/heading on divider to keep groups of folders (same topic, same year, etc) together
- Transfer box of folders to scanning work crew.

JOB COACH RESPONSIBILITIES

A. Job Coach Orientation and Training

1. Know each individual and the specific job he/she person performs in the scanning process.
2. Familiarize self with the job site and work space/station where scanning will be done.
3. Familiarize self with computer and scanner equipment that will be used.
4. Review/understand all steps in scanning process (See "Scanning Steps").
5. Orient self to new work site:
 - _____ Entrance where individual(s) (workers) arrive.
 - _____ Security sign in/sign out process.
 - _____ Accessible restroom locations.
 - _____ Lunch room/lunch area.
 - _____ Sick room.
 - _____ Vending machines.
 - _____ Evacuation procedures/exits from building
 - _____ Location of copier and how to track copies made (if necessary)

B. Job Site Expectations, Work Culture and Norms

1. Standards of conduct for the particular job site.
2. Dress code.
3. Personal phone calls – when/where.
4. Policies regarding computer and internet use/restrictions.
5. Breaks/lunch times (scheduled or flexible) and place.
6. Events/occasions that all employees participate in at the job site.
7. Know contact person(s) at job site and where/how to reach them for questions, scanning updates, supply needs.

8. Establish communication process with employer/contact person to include the following:
 - a. Notify contact person at least a week in advance when:
 - _____ Supplies needed (CDs, other supplies).
 - _____ Scanning of box(es) of folders will be completed
 - _____ Change of job coach
 - b. Notify contact person when a new individual will be coming to work, when individual(s) (workers) will not be on the job, or there is a job coach substitute/backup.

C. Daily Responsibilities

1. Arrive at job site before individual(s) (workers) arrive to do the following:
 - _____ Set up work space
 - _____ Review all folders and documents to be scanned that day
 - _____ Return copied pages to correct place in folder.
 - _____ Check supplies.

OR one or more of the above are part of the individual's job
2. Follow "Scanning Steps"
3. Meet individual(s) (workers) when they arrive and go to work station.
4. Go through orientation with all individuals who are new to the job and the job site, review the job that each person will perform, the environment in which he/she will be doing the job, and standards of conduct.

(Orientation check list for workers – include same items as for job coach orientation and training)

5. Individuals and job coach begin workday on time.
6. Follow "Scanning Steps"

7. Monitor scanning process and specific job that each person is performing.
- _____ Documents prepared for scanning (remove post-its, staples, paper clips)
 - _____ Document pages kept in order
 - _____ Single sided/double sided pages in documents
 - _____ Document pages placed correctly in scanner
 - _____ Scanned document pages returned to folder in correct order
 - _____ Scanned document pages returned to folder right side up

D. Other Responsibilities

1. At end of first week at new site (and as requested), burn a CD. (CD burning steps aren't included- specific instructions for different software is needed.)
2. Give the burned CD, paper list of folder titles and file titles, and folders with documents to job site contact person for quality check.
3. Return folders to box(es) and CD with paper list to job site contact person when scanning completed.

LABELING OF FOLDERS WITH SCANNED DOCUMENTS AND PREPARATION FOR TRANSFER TO THE HISTORICAL SOCIETY

Folder = paper folder

Document = paper document

1. Group folders according to approved records retention schedule. If you do not have an approved schedule, group folders containing documents of a similar topic/subject matter together.
2. Recheck title/name given to folder; use a uniform system, i.e. the description of the records series on the schedule or author.title. (date).
3. Arrange/sort in chronological order (unless another order makes more sense for future retrieval purposes).
4. Place folders (similar topic/subject matter documents) in storage/banker's box.
5. If folders containing documents of different topics/subject matter are placed in the same storage/banker's box, place a separator between the different groupings and note the topic/subject matter heading on the separator.
6. Complete the "Transfer of Records to State Archives" form (available at <http://www.mnhs.org/preserve/records/Transfer.PDF>). This will label the contents of the storage/banker's box with topic/subject matter and date range (if appropriate); if more than one topic/subject matter heading in a single box, note each clearly on the box label. Be sure to keep a copy of the transfer form for your records.
7. If transferring similar types of documents or an ongoing series of documents at various times (i.e. records of meetings that occur on a regular basis throughout the lifetime of an entity), keep the same topic/subject matter headings and same groupings.

NOTE: The Minnesota Historical Society (MHS) uses the naming system that the governmental entity uses and leaves documents in the order in which they are received (unless something is obviously out of place). The entity is responsible for establishing a system that makes sense to the entity, follows the retention schedule and facilitates retrieval.