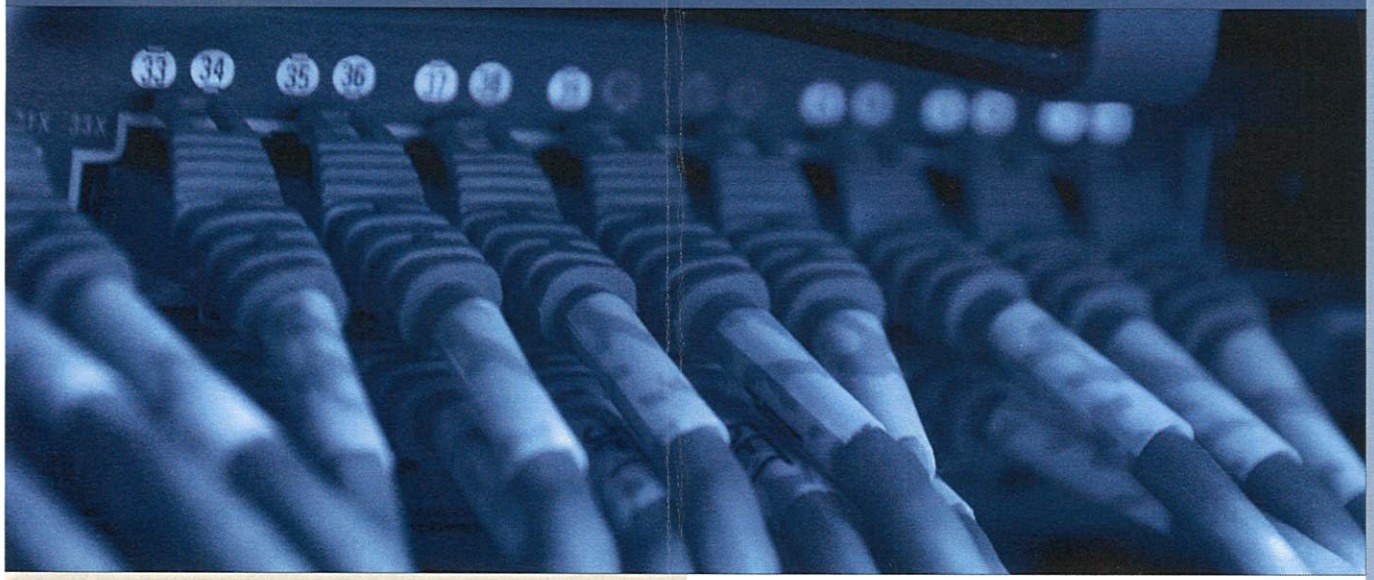
Effective data security starts with assessing what information you have and identifying who has access. Understanding how information moves into, through and out of your department or organization and who has – or could have – access is essential for identifying vulnerabilities.



OPPORTUNITIES FOR PROTECTING CONFIDENTIAL INFORMATION

1. INVENTORY

Track what personal information your department receives. Inventory all computers, file cabinets and other equipment.

Understand how your department uses personal information.

- Who sends sensitive information to your department?
- What sort of information does your department process?
- How does your department receive, send, or use sensitive information?
- Where do you keep sensitive information?
- When is the information collected, used, and disposed of?
- Who has access to sensitive information?

2. ASSESS NEEDS

Decide what information you need to do your job. Keep only what you need, and know how long it must be kept under the College's Retention Schedule.

Unless required to perform your job, do not collect the following types of information:

- Payment card information, such as credit or debit card numbers, expiration dates
- Government ID information, including Social Security numbers and State ID or Driver's license numbers
- Financial information, including bank account numbers or credit reports
- Computer account logins and passwords
- Student information, such as grades and evaluation information
- Health information, including medical charts or insurance information

3. SECURE INFORMATION

Take steps to protect the information you use in your job. Secure electronic media and paper documents in locked cabinets when not in use. Protect your physical environment, and remember to lock your workspace when away. Remember: an open door policy does not mean an open office policy.

Common steps include:

- Lock offices and facilities when away
- Lock your workstation (using Control+Alt+Delete sequence) when not in use
- Ask for ID before handing over sensitive materials to a stranger
- Carry your ID at all times, and report lost ID's immediately
- Record all outsider visits to sensitive areas
- Report misplaced or out of place items to superiors or The Department of Public Safety

4. DISPOSE OF INFORMATION PROPERLY

Sensitive information should be disposed of when no longer needed. The College's Records Retention Policy has established timeframes for the retention and disposal of information. Follow the policy directives for each class of record processed in your work area.

To ensure proper disposal:

- Destroy sensitive paper documents using a cross-cut shredder or shred service
- Electronic media, such as CDs, flash drives, and hard disks may be delivered to IT for proper disposal
- Paper documents pending destruction should be kept in a secured bin
- Clearly mark shred / destruction bins and trash bins
- Transient records that are no longer administratively necessary should be disposed of promptly