

## **MAINTAINING THE PHYSICAL SECURITY OF INFORMATION**

- is a critical piece of keeping confidential information and data secure.
- needs the attention of every user. Information is only as secure as the weakest link.

### **DO'S**

1. Lock your computer screen when you leave it (hold down control/alt/delete at the same time).
2. Lock your lap top, and secure it when it is not in use.
3. Use equipment locks that are provided. Though they may not be fail safe, they are a deterrent.
4. Keep paper or disks that contain confidential information secure in a locked storage area.
5. Shred confidential information with a cross cut shredder as soon as it is no longer needed.
6. Only print confidential information when needed, and keep it secure.
7. Use a cover sheet for faxing confidential information, and verify that your recipient is expecting it before sending, and that he or she received it. Ask others who fax you to do the same.
8. Make sure that when you are reviewing any confidential information (electronically or paper) that no one is shoulder surfing.
9. Return equipment to the appropriate staff person when no longer needed, so that it can be properly tracked and or disposed of in a secure manner.
10. If sending confidential information via a public carrier (i.e. UPS, U.S. Postal Service, it is best sent double-sealed in appropriate secure container, addressed to specific recipient with no special marking on outer container. This is especially important for electronic information where many records may be included (which should only be sent in an encrypted format).

### **DON'TS**

- Do not let people into the building or on the floor without identification and permission.
- Do not share your password or post passwords where others can view or find them.
- Do not leave confidential information in a phone message.
- Do not leave confidential information out where others can view it.
- Do not discuss confidential information in an area where others can overhear you.
- Do not leave confidential information for another user in an insecure location (i.e. on a desk).