

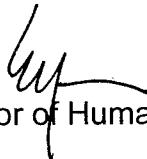
UNIVERSITY OF HAWAI'I

Office of Human Resources

MEMORANDUM

April 26, 2006

TO: Vice Presidents
Chancellors

FROM: Edward Yuen 
System Director of Human Resources

SUBJECT: Safeguarding Confidential Data

Due to increased awareness and the serious ramifications of identity theft, please ensure that adequate safeguards are in place to prevent the loss or compromise of hard and electronic copies of personnel documents. Such items include, but are not limited to, the following:

- Employee Personnel Folders

Civil Service employee folders are centrally stored at the Office of Human Resources (OHR). Physical security has been installed at the OHR to safeguard these hardcopy documents. Departmental offices are responsible for storing personnel data for Board of Regents' appointees. Please ensure that adequate measures are in place in the departmental offices to safeguard this data. Folders should be moved to secure locations if adequate safeguards cannot be maintained at the employing department.

- Electronic Data and Documents

Personnel data in PeopleSoft can only be accessed by authorized users. However, the ad hoc reporting tools Brio and Discoverer now make it possible for users in the field to download confidential information to their individual workstations. Workstations may also store confidential information related to grievances and disciplinary actions. While workstations should have login capabilities in place, please ensure that adequate safeguards are in place to secure these workstations from physical theft. If this is not possible, files stored on these workstations should be encrypted with a password. Additionally, users should logoff their workstations when absent for an extended period of time to minimize the possibility of unauthorized use or access.

- **Username and Passwords**

As additional on-line applications require a UH username and password or other login security information, please ensure that this information is not shared with other staff members. Your login security represents your electronic signature and is assigned for a specific employee.

- **Unwanted Intrusions**

Confidential information casually placed on desktops is a magnet for "wandering eyes." Please ensure that this information is properly stored and placed in a secure location when not being used.

- **Document Destruction**

Documents containing confidential information should be shredded at the appropriate time (see Administrative Procedure A8.450, Records Management Guidelines and Procedures). Confidential employee information in unshredded documents could be retrieved from dumpsters and trash cans.

- **E-mail is not Secure**

Do not use e-mail for sending confidential data. E-mail is unsecured and open for anyone watching traffic on the network. You should either encrypt e-mail before transmission or directly telephone the person if confidential information must be transmitted.

Priority should be given to insuring the proper use, handling, storage and destruction of confidential information. The theft of personal information may have long-lasting effects on an employee's financial position. Therefore, we must all do our part to ensure the confidentiality of employee data.

For further information on security issues related to electronic data, please contact Jodi Ito, ITS Security Administrator at <jodi@hawaii.edu>. For additional information related to the security of human resources documentation, please contact Steve Yamada at <syamada@hawaii.edu>.