



PRAIRIE VIEW A&M UNIVERSITY

A Member of the Texas A&M University System

April 30, 2010

OFFICE OF BUSINESS AFFAIRS MEMORANDUM No. FY10-74

Distributed via Campus Email

To: All Employees
From: Mary Lee Hodge, Senior Vice President for Business Affairs
RE: Data Security

Most offices on campus handle several items which include sensitive information, which should be kept confidential at all times. We must ensure that there is no data loss, or data theft. To prevent any such instances the following guidelines shall be followed strictly in order to guard this sensitive data:

1. Any data which establishes a correspondence between a name and social security number/UIN number/Student ID is defined as Sensitive Personal Information.
2. Sensitive Personal Information shall not be transmitted by any potentially insecure mode of communication, such as letters, emails or voice mails.
3. Sensitive Personal Information shall not be stored on removable drives or media such as memory sticks, flash drives, and external drives.
4. Supervisors of student workers are responsible for ensuring that students do not use flash drives to input/output sensitive Personal Information for any reason whatsoever.
5. Sensitive Personal Information shall be stored only on servers through mapped drives in the individual computers. They shall not be stored in office computers used by individual employees. They can be taken into such computers for working on, but should be returned to the servers at the end of the work session. It shall be ensured that no copies/duplicates remain on the individuals' computers.
6. As far as possible, no correspondence should carry sensitive Personal Information. If, in any type of letters, memos and emails, it is absolutely vital to establish a relationship between a name and the corresponding social security number/UIN number/Student ID, only the last four (4) digits of the relevant number should be given, and the preceding digits masked by a series of "X"s.
7. All staff shall familiarize themselves with the "Red Flag Rules" dealing with the prevention of identity theft. Link <http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.pdf> can be followed to locate these rules.

8. All staff who is working with Sensitive Personal Information must write procedures to ensure safe capture and transfer of such information to the mapped drives.

Breach of any the instructions above will result in progressive disciplinary action including and up to termination. Information security questions should be addressed to Mr. Louis Morgan via to lamorgan@pvamu.edu

xc: President George D. Wright
Mr. Albert Gee
Mr. Louis Morgan

MLH/alv