MIDWESTERN STATE UNIVERSITY

Information Technology

PII Data Handling and Storage Tips

Midwestern State University is responsible for the confidentiality and integrity of their data under existing federal and state legislation. Included in this document are some "best practices" for those handling Personal Identifiable Information (PII). PII as defined by Texas Business and Commerce Code Title 11, Subtitle B, Chapter 521 but is not limited to:

- Social Security Numbers (SSNs)
- Driver's License or State Identification Number
- Protected Health Information – including immunization information, FMLA information
- Financial Account Number – including credit/debit card

PII does not include publicly available directories containing information an individual has voluntarily consented to have publically disseminated or listed, including name, address, and telephone number and does not include information made lawfully available to the general public from federal, state, or local government records.

The following recommendations have been compiled to assist you in keeping University PII secure. Please follow these simple rules.

- **If you don't need it, don't store it**
  - Many offices retain forms of PII "just because". Review your processes and data retention policies. If you don't need it, don't keep it!
- **Secure your computer**
  - When leaving your office for any length of time, no matter how short, always lock your computer by pressing the Ctrl, Alt, and Delete keys simultaneously and select "Lock this computer" from the menu and press Enter
  - Use a password protected screen saver
  - Do not remove or alter your computer's antivirus application settings
- **Delete files from ALL locations (hard drive and network drive) when no longer valid**
  - Do not hold on to old queried or reports that contain personal information
  - Empty your computer's recycle bin and clear temporary file folders regularly
- **Never save or store files containing PII to the Z: drive**
- **Never share your user name and password with colleagues or students**
- **Avoid emailing sensitive files**
- **Avoid saving files that contain PII on CDs, DVDs, portable devices, etc.**

REMEMBER: It is every user's responsibility to protect data and to treat other people's information as if it was your own. Disclosure of PII can be used to steal identities, disrupt University operations and damage MSU's reputation.