According to a report published March 1, 2012 by Space.com:

“A laptop stolen from NASA last year was unencrypted and contained command and control codes for the International Space Station on it, the agency’s inspector general told a United States House subcommittee yesterday (Feb. 29).

In his testimony before a Science, Space and Technology House subcommittee, NASA Inspector General Paul K. Martin said the notebook computer stolen in March 2011 "resulted in the loss of the algorithms" used to control the space station. This particular laptop, Martin said, was one of 48 NASA notebooks and mobile devices stolen between April 2009 and April 2011.

Some of these thefts resulted in the leak of sensitive data "including export-controlled, Personally Identifiable Information, and third-party intellectual property," as well as Social Security numbers and data on NASA's Constellation and Orion programs, Martin said.”

Please remember that export controlled information and technology is Category I Data. See, Extended List of Category I Data, Item 5 – Research Data:
http://www.utexas.edu/cio/policies/pdfs/Extended%20List%20of%20Category-I%20Data.pdf

Pursuant to UT System Policy, all University-owned laptops as well as all personal laptops that contain Category I Data, must be whole-disk encrypted.

As a general rule, export controlled information should never be saved to or stored on a USB, flash-drive, thumb-drive, external hard drive, PDA, smartphone, or cell phone (including via email attachments).

If you need additional assistance, you may contact either your local IT support staff or the ITS Help Desk at 475-9400 or help@its.utexas.edu. Questions for the Information Security Office can be directed to security@utexas.edu.

Questions concerning Export Controls or Technology Control Plans can be directed to the Export Control Officer at 475-7963 or ivery@austin.utexas.edu.