MEMORANDUM

Thursday, October 04, 2012

TO: Dr. Pierce Cantrell 
Vice President and Associate Provost for Information Technology

FROM: Mr. David Sweeney 
Chair, Information Technology Advisory Committee

SUBJECT: Password Recommendations

Last year, an ITAC subcommittee investigated password policies at Texas A&M University, and recommended that those policies should be changed to meet industry standards and best practices. Dr. Henrik Schmiediche chaired the subcommittee with members Jim Rosser, Rick Young, Bill Chollett, Jeff McCabe and Willis Marti. The committee looked at three broad password related areas: password ageing, password complexity and password procedures. Attached is the final report of this committee with nine recommendations.

In summary, the committee found that the TAMU Password SAP is out of date with current best practices in all three areas, but particularly in the area of password ageing. Password ageing is generally not effective and should only be used as a risk mitigation of last resort, and then only on user accounts. Other risk migration procedures should be used whenever possible.

The committee made nine password related recommendations. Seven of these were:

1. No password ageing should be required on any information resource that can be moved offsite. Password ageing provides no benefit in these cases. Examples are encrypted files or portable devices.
2. Passwords that cannot be attacked remotely should never expire. Examples include desktops or laptops that have no remote access enabled or embedded passwords only accessible from the console.
3. Any password with sufficient complexity should never expire. Examples are randomly generated passwords often used in machine-to-machine interactions.
4. Password complexity should be required to eliminate default and obviously weak or short passwords, but password security should not be pursued through expansion of complexity rules. Good pass phrases are an alternative to complexity rules.
5. Multi-factor authentication should be encouraged. Password complexity and ageing requirements for multi-factor authentication systems should be minimal.
6. If countermeasures to remote “brute force” attacks can be put into place, then password-ageing requirements should be removed or greatly reduced to mandate less frequent password changes. Counter measures might consist of monitoring the number of remote attacks on a system, temporary lockout on multiple password failures, requiring multi-factor authentication on suspicious logins or locations, etc.

7. No password should expire in less than 24 months.

Recommendations 8 and 9 involved password procedures that are, for the most part, already in place. Please see the report for research and justification of these recommendations.

ITAC recommends that the Information Policy Committee examine these recommendations and make appropriate adjustments to rules and standard administrative procedures as soon as possible.