MEMORANDUM
Tuesday, November 20, 2012

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

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

SUBJECT: Password Reset Recommendations

Texas A&M employees who currently call Help Desk Central and request that their account be flagged for password reset incur more risk than those using the Self-Service Password Reset (SSPR) system. This is primarily because over-the-phone authentication is more susceptible to fraudulent actions, especially when the agent doesn’t know the person requesting service. Eliminating employees’ ability to call HDC to request a flag for password reset and moving to SSPR will increase security and reduce identity theft. ITAC supports eliminating an employees’ option to call HDC to request a flag for password reset and requiring all NetID users to use SSPR or in-person resets.

To help facilitate more confident identification of users, ITAC recommends development of an Identity Agent program. Like the HR Liaison program, this program should be required at the department, division, or college level, and would give local identity agents sufficient authorization to flag accounts for password reset for employees within their organization whose identity they can verify.

ITAC recommends the following:

- Implement a communications plan that details the reasons for moving to SSPR via Distribution A and memos to unit heads. These communications should come from VPAPIT, should emphasize the security reasons for not allowing accounts to be flagged for password reset over the phone, and encourage unit heads to mandate that employees in their area cannot call HDC to have their account flagged for password reset.
- Develop a reasonable timeline for units to eliminate their employees’ ability to call HDC to have their account flagged for password reset. Offer tools to help units make the switch such as unit-level account flagging, and routine communication templates sent to unit heads for distribution to their employees.
- Provide routine data to units about who has not set up SSPR.
- Create an Identity Agent program to train and authorize unit-level personnel to flag accounts for password reset. Although any fulltime employee could be identified as an Identity Agent (i.e., no students), IT or HR personnel are optimal choices; IT personnel are accustomed to operating after-hours and are familiar with information systems, and HR personnel have access to systems with data that will allow them to verify a person’s identity.
- Implement a default setting for all incoming students and employees that does not allow them to call HDC to have their account flagged for password reset over the phone, and requires SSPR to be set up immediately.
- Include SSPR in annual security awareness training.