Objective: In order to comply with the University of Tennessee’s information technology policies and industry best practices, new functionality has been added to ANDI that provides for password complexity, password expiration and an anti-hacker feature that locks a user account after 5 invalid login attempts.

Password Complexity:
ANDI passwords must be at least eight (8) characters but no longer than twelve characters. The password must include at least one numeral, one non-alphanumeric value (e.g., a punctuation mark), one upper case letter and one lowercase letter.

Password Expiration:
ANDI passwords will expire every ninety (180) days. A warning message indicating how many days remain until their password expires will be sent to each user beginning 14 days ahead of the actual day of expiration. This message will display each time a user logs on to ANDI until the password is changed or expires. If a user attempts to login after the password has expired, the attempted login will take the user directly to the “Change Password” window.

User Lockout:
A user will be allowed five (5) invalid logon attempts within a thirty (30) minute period. After 5 unsuccessful attempts ANDI will lock the account. If a user account is locked, the user must contact ANDI Help at 865-974-4153.

For questions regarding this policy, contact the Advancement Services help desk at (865) 974-4153 or email ANDIHelp@tennessee.edu