College of Arts and Architecture
Password Policy

This policy states the password requirements for systems in the College of Arts and Architecture. These requirements are enforced by default on all deployed systems and locally controlled network accounts where able. These requirements directly follow the requirements of Penn State University ITS as detailed at http://its.psu.edu/be-safe/password-policy/ and policy ADG02, any updates of which can supersede this policy.

Desktop and Server Account Passwords

The following are required on any system image deployed after March 2010 and all A&A servers with locally hosted accounts, including Open Directory masters and accounts created by A&A IT staff in the CAA OU in the PSU AD. For systems not using the college base images with these policies in place, these rules must be locally enabled by hand by the IT staff.

- Passwords must contain at least 8 characters
- Passwords must contain at least one alphabetic character
- Passwords must contain at least one numeric character
- Passwords can not contain the user name
- Passwords expire and must be changed every 12 months
- Passwords can not match the previous 5 passwords used

The following are strong recommendations to all users, but the password policies of the systems are not set to enforce these. At the user's request these can be enabled by default on individual systems.

- Passwords should contain one non alphanumeric character
- Passwords should not contain any proper names or words
- Passwords should contain upper and lower case alphabetic characters

At this time systems are not set to lock accounts after a number of failed login attempts. As this is recommended by security audits, this may change and this policy will be updated accordingly. Historically this has been avoided due to hacking attempts and other configuration issues causing accounts to be locked out daily if it was enabled. At such time as network firewall security and system configuration prevents this, the practice will be re-examined.

At this time desktop systems are not configured to disable accounts after a period of non use. Server based accounts like Open Directory are configured to disable accounts after a maximum of one year of non use.

Domain Passwords

All of the above considerations are enforced by the university for domain accounts, and as such any computer or server file share using domain (PSU AD) logins is in compliance with policy.

BIOS, EFI and OF Passwords

Hardware level passwords including BIOS, EFI, and Open Firmware are to be set by AAIT for system security and must follow the above account password rules. As there is no method of enforcing this, the onus is on the IT staff to be in compliance with the policy. All systems should have these passwords set.

Password Security

Users are bound by university policy to never share account password information with anyone. IT staff can report infractions of account security to the College and University Accounts Office. Administrator account and boot level passwords set by the IT staff will be kept on file in sealed envelopes in a safe locked in the Borland server room in the event of emergency.

Account Security

All users will follow the guidelines of least privileged access. In the event a user (including IT staff) has an account with administrator level rights, this account will not be used under normal circumstances. All users will have an account with user level access that is used for daily operation. This includes local and domain level accounts.

On any system that has a guest account, that account will be renamed to something other than guest (if possible) and disabled, or if possible deleted entirely.

Administrator accounts should not contain the word admin or other obvious words that indicate the access level of the account. This means built in accounts may need to be renamed. It is highly suggested that the account name follow the pattern of a PSUID so as to be indistinguishable from a user account. It must be verified that such a name does not conflict with an actual PSUID.

On Mac systems, the root account should not be enabled but should have a password set on it.