ODP Computer Security and Password Protection Policy

For accessing all computer server systems within OOP, there are three (3) required levels of protection plus an optional level on some workstations. Format specifications are provided to users to indicate maximum length of password, characters that can be used, and a recommended minimum length as well as cautions to observe when choosing a password.

Level 1

This level controls the access to the modem bank for those users who dial in from a telephone line. All users dialing in must have a password to gain access to the resources located at ODP. For those users who access a server system via the internet, unless using common HTTP, access must be granted through TAMU's firewall. In addition, passwords are required for the access to data, which is considered to be protected.

Level 2

This level controls access to each of the servers which are available. A user accessing a server must have a valid username and password to gain access.

Level 3

This level is used to protect certain data from access by everyone permitted to be on a given server. To access protected data, the user must have a valid password which gives authorization to access the data.

Optional Level

Most workstations have operating systems and applications which will support password protection not only to gain general access, but also for protection of individual applications and data files which the user desires to protect. This level of security is left up to the user. Users who have sensitive data on their systems are advised to utilize this capability.
Be aware that an automatic timeout feature is implemented on some servers such that inactive users are disconnected.

Account Authorization

Accounts and permissions to facilitate the above are only granted upon the receipt of a completed New Account Request form, which can be obtained from your supervisor, the ODP ISD Helpdesk, or at: http://www-odp.tamu.edu/isg/new_account.pdf

General Advice

Some systems enforce password standards, such as mixture of letters, numerals, and punctuation characters, minimum length, or automated password expiration/replacement. Please select passwords accordingly. It is ALWAYS an excellent idea to select or to construct a password that is at least 8 characters in length, that consists of a mixture of character types, that is not in any way derived from your personal life, and that does not occur in any dictionary in any language.