

Frequently Asked Questions

ITS will begin implementing an OMB mandated stronger password policy on **Friday, February 1, 2008, after 9 p.m., EST**. The policy will apply to all computers using the Windows XP Professional Operating System and joined to the End User Computing domains (AGEAST, AGWEST, AGCENTRAL, AGLO and ONE). The purpose of the stronger password policy is to reduce overall security and privacy risks to the ITS End User Computing Environment that result from weak passwords.

This means that your LAN password must now:

- Be at least 12 characters in length;
 - Contain characters from each of the following character types:
 - Upper case alpha (A through Z)
 - Lower case alpha (a through z)
 - Numeric (0 through 9)
 - Special characters (e.g., ! @ # \$ % ^ & * etc.)
 - Will expire every 60 day; and
 - Cannot be the same as any of the 24 previously used passwords.
-

Who do I contact if I forget my password or get locked out?

If you make 5 invalid logon attempts, your user account will be locked out. However, the lockout duration is for 15 minutes after which you can attempt to logon again. If you have forgotten your password and need it reset to a temporary password, follow normal support procedures.

Will I be required to change my password on February 2, 2008?

It depends on when your current password expires. For example, if you created a new password on January 28, 2008, you will not be prompted to create a new stronger password until 45 days (60 days – 15 day warning that password is due to expire) have passed. If you last changed your password in late December, you will be advised at your next login that the password has expired and you will be required to create a new stronger password.

Which passwords are affected by this policy?

Only the passwords used for computers that are owned and supported by ITS in the End User Computing Network. This policy does not affect passwords for USDA e-Auth, WebTA, NFC, FFIS, STARWeb, FedTraveler, etc.

Who issued the policy?

The policy is mandated in Office of Management and Budget (OMB) Memorandum M-07-11 (Implementation of Commonly Accepted Security Configurations for Windows Operating Systems) and by the USDA CFO/CIO Memorandum (USDA Password Policy, December 14, 2007) and covers all computers using the Microsoft Windows XP and Vista operating systems.

What is the purpose of this policy?

Passwords are the most common means of authentication and strong passwords are a simple and effective way to improve network security and reduce overall security and privacy risks to the USDA user community. Studies by the National Security Agency (NSA), the United States Computer Emergency Readiness Team (US-CERT), and the SANS Institute have shown that weak passwords are serious security vulnerability.

How do I create a strong password?

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters, for example:
0-9, !@#\$%^&*()_+|~=\`{ } [] : " ; ' < > ? , . /
- Are at least twelve (12) alphanumeric characters long and is an easy to remember pass phrase, such as “Ohmy1stubbedmyt0e” for the phrase “Oh my, I stubbed my toe.”
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, pets, friends, co-workers, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "I love my great aunt's sweet ice tea and apple-peach cobbler 2."