

Mid South Area

Computer Support Newsletter

Email all questions and comments to: MSA-HelpDesk@ars.usda.gov

Employee Personal Page (EPP) and Thrift Savings Plan (TSP)



The Area IT Office nor anyone at your Location can access or reset your Employee Personal Page (EPP) ID or password nor can they reset your Thrift Savings Plan (TSP) ID or password. Both systems are covered by the Privacy Act.

EPP is a separate system from TSP. Prior to the end of calendar year 2007, TSP account IDs were mailed to employees via the US postal service. The TSP website is: <http://www.tsp.gov/account/index.html>. Frequently asked questions may be found at: <http://www.tsp.gov/faq/index.html>. TSP contact information may be found

at: <http://www.tsp.gov/curinfo/contact.html>.

ARS Employees received an [NFC Bulletin](#) via email on or near February 19, 2008. The Bulletin outlines changes made in accessing EPP at the National Finance Center. The attachment at the end of the [NFC Bulletin](#) outlines particular requirements for setting User ID and Password. After you have successfully logged in to your EPP, you may then use your E-Authentication/AgLearn credentials to login. The EPP web site is: <https://www.nfc.usda.gov/personal/index2.asp>.

Employee Personal Page Contact Information:



Email Requests to: occ.etix@usda.gov



Submit requests via phone to: **1-800-767-9641** or **504-426-6435**

Inside this issue:

- Employee Personal Page (EPP) and Thrift Savings Plan (TSP)
- E-Vault is on the way...
- Authentication
- Three Types of User IDs
- Password Attributes
- ARSNet Passwords
- ARSNet Password Resets
- Useful Tips and News
- Cyber Security Awareness

E-Vault is on the way...

Symantec Enterprise Vault (E-Vault) services will be implemented across ARS in the coming months. E-Vault is a system that allows email messages to be archived automatically to a server. E-Vault will provide the following services to our Outlook email users:

- Archive Outlook Inbox and subfolders, except for "Deleted Items"
- Enable users to access archived messages using Outlook Web Access
- Archives backed up centrally and safely
- Powerful search tools for finding archived files quickly
- Archived messages can be Forwarded, Deleted, Replied to



Authentication

According to *Webster's* dictionary, authenticate is, "to prove or serve to prove the authenticity of, as in *authenticate* a document."

The authentication process is an important process used to establish whether or not an authorized user is operating a given system, and if so, what their level of access is. It is the current means of insuring only authorized access to U.S. Government Computer Systems.

Within the concept of the ARS, authentication means a user ID and password is used to prove the identity of an authorized user. The user ID and password alone are what is referred to as single factor authentication. They are only useful as a set. The ID alone, or the password alone are meaningless as proof of who a user is.

It is critical to associate the correct system with its proper user ID/password set.

There are only a few systems which use the same user ID and password:

USDA e-Authentication account:

- AgLearn
- Employee Personal Page (requires e-Authentication setup)
- GovTrip

ARSNet:

- Outlook
- SharePoint
- eForms
- REE Updater

The e-Authentication user ID will consist of 6-20 characters.

The ARSNet user ID is in the format:
arsnet\firstname.lastname

Three Types of User IDs

1. System Fixed

- Examples are user "Administrator" for every default copy of Windows XP software.
- Advantages/disadvantages: Easy to guess and could be used to gain unauthorized access if password is nonexistent or easily guessed.
- Most appropriate for low to no security environments

2. Cryptic

- Examples are: AR0123
- Advantages/disadvantages: Difficult to guess and easily forgotten or confused with others.
- Most appropriate for higher security environments and places with high rate of employee turnover.

3. Meaningful

- Firstname.lastname@ars.usda.gov
- Advantages/disadvantages: Easy to remember and easy to guess. Can be confused with other information such as arsnet\firstname.lastname@ars.usda.gov in the improper context
- Most appropriate for low security environments.

Password Attributes

1. Length: The number of characters. Security wise, the longer the better, but many NFC systems accept a maximum of 8 characters and USDA's e-Authentication requires 9 characters.
2. Complexity: Generally pertains to uppercase/lowercase letter, numbers, and special characters.
3. Age: Is usually expressed in days. Many systems have maximum ages which range from 30 to 90 days. When the maximum age is reached, you must change the password, or you will be locked out of the system.
4. Ability to reuse passwords: Generally not allowed.
5. Force Change at Login: A way to make password known *only* to users. User passwords are stored in such a way as to make them unusable even by the systems administrator. A user's systems password is generally not known to the administrator.
6. Number of failed attempts before lockout is the means to prevent password guessing.

Helpful password information can be found at this site:
<http://usewisdom.com/computer/passwords.html>



ARSNet Passwords

The password minimum complexity requirements for ARSNet are:

- Contains at least 8 characters
- Contains at least three of the four character groups
 1. English uppercase characters (A-Z)
 2. English lowercase Characters (a-z)
 3. Numerals (0-9)
 4. Non-alphabetic characters (such as ?, \$, #, %)
- Does not contain your account or full name
- Has not been used in the previous 8 passwords

Your new password must be more than 7 days old before you can create a new password.

Password expiration notifications are emailed to ARS employees who:

1. In the last three months (at least once), have used either ARS intranet-SharePoint, Outlook Web Access, Outlook Client, e-Forms, or REE Directory (Updaters only)
2. Accounts must be active (not locked or disabled)
3. Password is not already expired
4. Accounts do not have apostrophe in either first or last name



ARSNet Home

<https://arsnet.usda.gov/default.aspx>

ARSNet Passwords Resets

To have your ARSNet password reset, please notify your location contact.

- Auburn—Betty Shepherd
- Baton Rouge—Gail Champagne
- Bowling Green—Jason Simmons
- Lexington—Gary Schaeffer
- Mississippi State—Gary Burrell
- New Orleans—Hans Wientjes
- Oxford—Tyrone Swearengen
- Poplarville—Susan Herrin
- Stoneville—Kathi Tullos

You are **not** allowed a grace login for an expired ARSNet password. Once your password has expired, you cannot access your account until your password is reset. You will be required to call your location contact to have your password reset.

If you do not read your email on a regular basis, mark your calendar and remember to reset your password **BEFORE** it expires.

“Good understanding and the discipline to manage User IDs and passwords will increase productivity of both the user and IT support contacts.”

Useful Tips and News

Learn More About Outlook

The MSA IT office has provided a place for you to find information on Outlook. Log into the Migration SharePoint site and then click on “100 Tips for Using Outlook.” You will use the same ID and password as you use to log into your email. Click [here](#) to give it a try!

Avoid Copyright Infringement

Copyright infringement occurs when you use or distribute information without permission from the person or organization that owns the legal rights to the information. Including an image or cartoon on your web site or in a document, illegally downloading music, and pirating software are all common copyright violations. While these activities may seem harmless, they could have serious legal and security implications. [Read more.....](#)

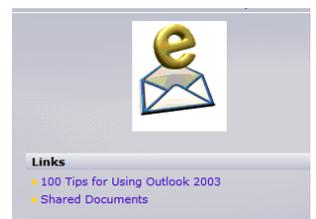
Vista, iPhone and Office 2007

Until a working plan or a new moratorium is in place, consider last year’s moratorium on utilizing Vista to still be in effect.

The Department’s iPhone ban is extended through September 30, 2008.

Office 2007 is incompatible with Office 2003. A “plug-in” is required from Microsoft that has not been fully tested and validated.

Supporting these new products would be difficult as IT staffs have not been fully trained and introduced to these products.



<https://arsnet.usda.gov/sites/MSA/migration/default.aspx>



Cyber Security Awareness

2008



“Protecting and Safeguarding Information”

10 Key Things Every Employee Should Remember

- ***Personally Identifiable Information (PII): Protect It Like Your Own***
- Keep your password to yourself. Don't share your password with anyone, including help-desk personnel. Do not store any privacy or PII data on your computer unless it is encrypted.
- Do not open emails that appear suspicious or sent by persons you do not know. Delete such emails immediately.
- Know how to contact your agency Information Systems Security Program Manager.
- Report lost or stolen equipment and PII to 1-888-926-2373.
- Safeguard your information and your customers' data.
- Never provide critical computer information to just anyone. Only provide critical computer information to OIG, agency ISSPM, or USDA OCIO Cyber Security.
- Do not install/use peer-to-peer software, download or distribute copy-righted materials, copy or use unlicensed software. Do not install any software without approval of your computer contact.
- Do not move sensitive data to unencrypted external storage devices (i.e., USB flash drives).
- A security clearance is not an authorization to see all information. Before sharing sensitive information and data, make sure the message receiver has a valid need to know.

If you have any questions, contact your Area IT Specialist at MSA-HelpDesk@ars.usda.gov

Sponsored by: The Office of the Chief Information Officer