AES Branch,
Foreign Trade Division

AES*Direct* Account Maintenance Changes

June, 2008

Changes Effective October 1, 2008

AES*Direct* Plans to Implement Increased Security Measures

Effective October 1, 2008, AES*Direct* will have heightened security measures and user authentication practices that will further increase the level of protection offered to its users. These changes include:

- **Individual User Account Administration**
- **Stronger Password Requirements**
- **Shorter Password Expiration Timeframes**
- **Automatic Inactive Account Deactivation**
- **Session Timeout/Concurrent Login Limit**
- **Account Lockout after 3 Unsuccessful Logins**
- **New Account Administration Functions**

AES*Direct*'s Increased Security Measures Benefits its Users!

Special points of interest:

- ✓ Stronger passwords
- ✓ Individual User Accounts
- ✓ Automatic Account Deactivation
- ✓ New Administrative Functions
- ✓ Shorter Password Life Spans
- ✓ Account Lockouts

All of these changes fall under Department of Commerce's security guidelines and address the U.S. Census Bureau's IT Security Program Requirements. The upgrade to the AES*Direct* system will provide AES*Direct* users with the utmost in user and account security. Each change will be explained in detail in the pages to follow. As always, AES Client Support is available to assist you with any issues/questions that you may have. Please call 1-800-549-0595, option 1 or e-mail askaes@census.gov if you need further assistance or clarification.

Keep in mind, these changes will not go into effect until October 1, 2008.

First Things First… Individual User Account Administration

Currently, when a company registers with AES*Direct*, an Administrator Account is created. The Account Administrator then creates a username and password that is utilized company-wide regardless of the number of users. The Administrator changes the password every 180 days and disseminates new password information to all users.

With the new security implementation, each company will continue to have an Account Administrator; however, every user of the system within the company will be required to have their own username and password. The Account Administrator will be responsible for maintaining accounts at the user level and will be responsible for performing various administrative functions.

New Password Requirements

AES*Direct* has changed the requirements on all passwords to make the passwords **"stronger."** The strength of a password relates to its effectiveness as an authentication tool and refers to its length, complexity, and randomness.

Protect Your Password!!!

The new requirements for AES*Direct* passwords are as follows:

- Passwords must be at least 8 non-blank characters
- Passwords must contain characters from 3 of the following 4 character classes
  - Lowercase letters
  - Uppercase letters
  - Digits
  - Non-alphanumeric characters (!, $, #, %)
- Passwords must contain the following:
  - At least 1 character must be alphabetical and at least 1 character must be a digit or a non-alphanumeric character
  - At least 6 characters must occur only once in the password
  - Passwords must be unique for 2 years
  - Passwords must be unique within the last 8 passwords
  - Passwords cannot contain any string that is also contained in the username
  - Passwords cannot contain any dictionary words
  - Passwords cannot contain any common strings such as
    - A sequential series of letters (eg. abcd)
    - A sequential series of numbers (eg. 1234) or pattern of numbers (eg. 2468)

Test Your Understanding

Under the new requirements, which of the following passwords are deemed acceptable?

1. 1234abcd	**2. Amg#94lm**
3. Today12!	**4. tmDmy12!**
5. $tay4A33	**6. 1!ife287**

*****Remember that dictionary words and common strings WILL NOT be allowed!**

Answers: 2, 4, 5, 6

Password Expiration

All system passwords have new expiration timeframes as follows:

- Passwords on standard user accounts will expire **every 90 days**
- Passwords on privileged (system admin/census/support) accounts will expire **every 30 days**

Time is of the essence!!!

Account Inactivity

Inactive accounts are now subject to the following guidelines:

To keep your account active, be sure to log in at least once every 45 days!!!

- After 45 days of inactivity, accounts will be deactivated
- Warnings will be sent once a day to any account that has been inactive for more than 40 days
- To reactivate an account the Account Administrator must contact AES*Direct* Support who will verify authenticity of the request and reactivate the account and administrative user.

Session Timeout/Concurrent Logins

All AES*Direct* sessions will time-out after 30 minutes of inactivity

- Users will receive a pop-up warning 5 minutes before timing out that will allow the user to click a button and remain logged in.
- If users are inactive for more than 30 minutes then they will be forced to login again. **All data from session will be lost.**

There will also be no more than 3 concurrent sessions allowed at one time (per login).

Account Lockout

All AES*Direct* users will be granted 3 consecutive invalid login attempts during a 24-hour period before being automatically locked out of the system

- Locked out users cannot be reactivated for at least 15 minutes

*****All locked out users must be reactivated by the Account Administrator.**

AES Branch,
Foreign Trade Division

www.census.gov/aes

Phone: 800-549-0595
Option 1 - AES Branch
Option 2 - Commodity Analysis Branch
Option 3 - Regulations Outreach & Education Branch

We're here to help you!!!

Our Pledge to You...

We understand that these new changes have the capacity to impact your work environment drastically and we are here to assist you in any way possible to provide for a smooth transition. If you have any concerns or encounter any issues that we are able to assist your company with as we migrate to the new security platform, do not hesitate to contact us via the information provided to the left.

Keep in mind user security, confidentiality and data integrity are our top priorities and we are here to serve you. Change can be overwhelming and we are aware of the effect this will have on your processes. The utmost concern for you, our clients, was taken into consideration as we developed and employed this new standard.

New Account Administration Functions

The following functionalities will be provided to the **Account Administrator** when the new Security measures go into effect **October 1, 2008**:

- **Create New User**
- **Search/View Users by:**
  - Name
  - Username
  - E-mail Address
  - Group (user level)
- **Edit User**
  - Change groups
  - Update profile (name, e-mail address, etc.)
- **Disable User**
- **Reactivate User**
  - This function will be used for manually disabled users and users that have been locked out. It will issue a reset code for the Account Administrator to give to user
- **Reset Password**
  - This function will issue a reset code that the Account Administrator will give to the user

The Account Administrator has the power!!!