Monday February 11th you will begin receiving the “Local Account Report” which summarizes the status of local accounts on domain joined computers in your unit(s). The purpose of the report is to assist IT Managers in preparing for the upcoming System Audit by providing awareness of existing local accounts with the idea that any accounts will either be removed or modified to comply with the same standards as domain accounts in regard to inactivity, password complexity, password age, etc.

Please note that computers not joined to the domain are not included in this report. However, those computers are subject to the same review as domain joined computers so it is recommended that all computers be reviewed for local accounts.

The report will be provided weekly for the first few weeks as audit preparations are in motion. Thereafter, it will be sent on a monthly basis. You will be notified prior to this change taking place.

Below is the email message that will be included with each report and a sample report is attached. Similar to the sample the actual report will be a pdf attachment.

Please review the information provided and let us know if you have any questions.

Thanks,

Tom

Tom Lyster
IT Coordinator
College & Research
Agrilife Information Technology
College Station, TX 77843-2468
Phone: 979-845-1439
Email: tlyster@tamu.edu

LOCAL ACCOUNT REPORT:
AIT is providing, on a weekly basis (initially every Monday and later on a monthly basis), a summary of the local accounts on domain joined computers in your unit. The purpose of the attached report is to assist IT managers in their preparation for the upcoming system audit by providing awareness of existing local accounts with the idea that any accounts will either be removed or changed to comply with the same standards as domain accounts in regard to inactivity, password complexity, password age, etc. Criteria in the report include:

1. Account is disabled? : True or False
2. User can change Password? : True or False
3. Password can expire? : True or False
4. Password Age (in days)
5. Must Change Password : True or False
6. Password is Required : True or False
7. Last Login Date
KEEPING A LOCAL ACCOUNT
If an account is to remain on the computer then it must be configured to ensure that the password is changed, expires every 6 months and that the owner utilizes this account per the standard account inactivity criteria of a domain account.

NOTE: All accounts that have been inactive for 120 days or more should be disabled. All accounts that have been inactive for over 150 days should be deleted upon notification to the Account owner.

KEEP OR REMOVE ACCOUNT?
Below are general guidelines to follow when reviewing the local account report. Please note when removing an account to be sure and safeguard any associated data unless the owner specifies it can be deleted.

1. If the account belongs to an employee who is no longer with the organization an account removal must be performed as per agency or college rules and procedures.
2. If the account is not actively utilized or needed by the owner remove the account.
3. If the account is a GUEST account it must be disabled. (Any activities associated with the Guest account, such as new employee hire paperwork, can be tied to an account other than Guest.)
4. If the account is an administrator account either
   - Remove the administrator account and rely solely on OU administrator credentials to maintain the computer
   - Rename the administrator account so it does not include admin or administrator in the name and configure the account parameters to meet domain account standards
5. If the account is the Sophos download account (typically named SophosSAU...) remove the account. It is leftover from an older version of Sophos and no longer needed.