Generic Account Policy

The Generic network accounts doesn't provide the university with any personal accountability with this type of account and therefore is a violation of best practices IT standards. It is the objective of the Technical Services to assure proper internal controls are in place, to safeguard University of Arkansas at Pine Bluff's assets. Therefore, effective immediately the Generic Account Policy is established.

PURPOSE

This policy establishes the process of creating and maintaining generic accounts for network, email and system access, on all of University of Arkansas at Pine Bluff's systems.

A generic account is any network account that may allow multiple users to use a single account to log on to the network or an account created in order to generate a specific email address. Any network account not created for a specific person using the Faculty, Staff or Student naming convention, is considered to be a generic account. There is no corresponding real user associated with a generic account.

ESTABLISHMENT AND USAGE

However, in some situations to support the functionality of a business process, system, device, or application, a shared account may be justified.

Desktop Computers on Campus / Network Login - Students, faculty, staff, and administrators must use their own network account when logging into computers in the Libraries, computer labs, and classrooms. Generic account use is limited to guests who are not affiliated with University of Arkansas at Pine Bluff. Every active student and current employee has a network account.

As network security depends on personal accountability and generic network accounts do not provide this, generic network accounts are forbidden. Users should submit a TS Job Request when requesting a generic network account for your area.

Local generic accounts are permitted. A local generic account is created on the workstation itself. It will not be able to access network resources, but it will have Internet access and will be able to run the applications installed on that computer.

Generic accounts created to generate an email address will be limited and can only be used to login to the online Outlook Web Mail system or to be added to outlook as an extra mailbox.

Any other generic accounts that do not fit these three scenarios will have to be approved on a case by case basis.

PROCEDURES

1. Generic accounts will be used by UAPB in cases where multiple users must access one workstation or application to perform assigned duties or temporary work.

2. The Technical Services process of submitting a TS Job Request must be followed to request the creation of a generic account.

3. Each generic account must have a designated owner who is responsible for the management of access to the account.

4. Each generic account must have a short description of the business case requiring the creation of the account.

5. Documentation must be maintained by the owner, which will include a list of individuals who have current access to the account.

6. The account password must be changed promptly whenever individuals accessing the account are terminated for any reason, or are transferred to a role that does not require access.

7. Network generic account access to workstations will occur only in protected areas where public access is supervised and/or restricted and the account may not be used on workstations in any other area.

8. Requests for all generic accounts will be reviewed and approved or disapproved by the Director of Technical Services.

9. Generic accounts will be audited on a regular schedule for appropriateness of access and ongoing need.

MAINTENANCE

All generic user accounts must be given the same attention as UAPB accounts and be de-provisioned when no longer needed. These accounts must be validated by the requestor associated with the account at the time of audit. If the audit results in it no longer being needed the account will be deleted by Technical Services.