LANDER
UNIVERSITY

Information Technology Services
http://www.lander.edu/its
help@lander.edu
864.388.8234

Departmental and System Accounts

I. INTRODUCTION

There are occasionally business needs that warrant shared access to an account (local or Active Directory), such as a departmental email account or a local account used to access a specific system. Such accounts are subject to many of the requirements stated in the Lander Account Password Policy, but some exceptions are established below to address the shared nature of these accounts.

II**. ACCOUNT CREATION AND ACCESS**

New departmental and system accounts will be created only upon the request of the appropriate Unit Head. Unless specified otherwise, the Unit Head will be the owner of the requested account. When there is a legitimate business need for shared access to an account, the Unit Head or authorized account owner can request that access be granted to another employee. This request must be documented and the access approved prior to the sharing of any departmental or system account credentials.

Existing accounts will be reviewed annually by ITS to verify that the account is still needed and confirm the accuracy of each account's authorized users.

III. PASSWORD POLICY COMPLIANCE AND EXCEPTIONS

Departmental and system account passwords are subject to the same expiration and minimum complexity requirements as stated in the Lander Account Password Policy. Such passwords must never be the same as a password for any authorized user's personal Active Directory account.

In the case of departmental and system accounts, credentials must only be shared, if necessary, with users who have been authorized by the appropriate Unit Head or account owner. If no additional users have been authorized to access the account, the sharing of credentials with any other user is prohibited.

In the event that an authorized user of a departmental or system account leaves or is terminated, the password for any account to which that user has access must be changed immediately. If no other authorized users exist, the appropriate Unit Head may take ownership of the account, designate a new account owner, or request that the account be deactivated.

IV. INAPPROPRIATE USE

Misuse of a departmental or system account is subject to the same disciplinary actions stated in the Technology Acceptable Use policy.

V. RELATED DOCUMENTS

Technology Acceptable Use Policy
Lander Account (Email / Active Directory) Password Policy
Password Creation and Protection Guidelines

VI. HISTORY

Created 1/3/2018
Reviewed by ITS 7/29/19