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

Lander Account (Email / Active Directory) Password Policy

I. INTRODUCTION

Information Technology Services (ITS) will assign Active Directory account credentials (username and password) to all users of Lander University information technology resources. Active Directory credentials will grant authorized users access to systems or services, such as Lander email, MyLander, Banner 9, and Bearcat Wireless. Since passwords serve as the first line of defense against unauthorized access to Lander University data and information technology resources, all users must adhere to this policy and take appropriate steps to safeguard any assigned Lander password and the systems/services accessible with that password.

II**. PURPOSE**

The purpose of this policy is to establish requirements for the creation, protection, and management of Active Directory passwords used by authorized individuals to access Lander University information technology resources.

III. POLICY

All default and user-created Active Directory passwords must conform to the minimum requirements defined in Section IV. Default passwords are generated during the creation of new Active Directory accounts and must be changed upon the user's initial login.

Users are responsible for protecting any account entrusted to them by the University. Safeguarding such accounts requires the creation of a strong, compliant password and the protection of that password's confidentiality.

Passwords to personal Active Directory accounts must not be shared with anyone. All passwords are to be treated as confidential Lander University information, and knowledge of an account's credentials does not constitute authorization to access that account or act on behalf of the authorized account owner. Users are responsible for any activity performed by their assigned Active Directory account.

Any violations of this policy will be subject to disciplinary actions up to and including loss of account access and termination.

IV. MINIMUM REQUIREMENTS

All Lander University Active Directory passwords must meet or exceed the following minimum requirements:

- Must be at least 10 characters in length
- Must include at least one letter and one number (special characters are allowed)
- Must not include (in full or in part) the individual's name / username or the University's name / mascot
- Must not be a common or previously compromised password (see Section VI)
- Must not be one of five previously used Active Directory passwords

V. EXPIRATION

All Active Directory passwords will expire after 365 days if no change or reset has occurred. Once a password has expired, each user must immediately change the password in order to regain access to their Lander account.

VI. BANNED PASSWORDS

A blacklist of banned passwords is enforced to prevent users from selecting a common or previously compromised password. Any attempt to use a blacklisted password for an Active Directory account will be rejected.

VII. RELATED DOCUMENTS
Technology Acceptable Use Policy
Departmental and System Accounts
Password Creation and Protection Guidelines

VIII. HISTORY
Created 9/16/16
Revised by ITS 1/18/18
Approved by Board of Trustees 2018
Reviewed by ITS 7/29/19