CLARK ATLANTA UNIVERSITY

Policy 14.5 Password Policy

CLARK ATLANTA UNIVERSITY		
Policy and Procedures	**Subject: Password Policy**	
Department: Office of Information Technology and Communications (OITC)	**Review Date:** 06/04/2020 **Effective Date:** 06/15/2020	**Issued By:** Chief Information Officer
Distribution: All University employees	**Required Approval:** University President	**No. of Pages:** **4**
Signature: Original signed by George T. French, Jr., Ph.D.		**Date: 06/15/2020**

14.5 Password Policy – Clark Atlanta University

TABLE OF CONTENTS

14.5 Password Policy – Clark Atlanta University

1.0 Policy Statement

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

2.1 Procedures Narrative

2.1.1 **Username/Passwords/PINs Assignment**

2.1.1.1 Faculty & Staff PantherID: accounts are established upon hiring or written request to OITC from Human Resources. The Username will be the individual's first initial and last name (unless previously assigned at which point an agreed alternative will be designated). A generic password will be assigned and the user will be prompted to change the password upon initially accessing the system.

2.1.1.2 Faculty & Staff Banner Web Accounts: accounts are established automatically upon hiring and users will obtain their account information from Human Resources (faculty & staff) or the Registrar's Office (faculty). The Username is the individual's ID (900#), and the PIN is an assigned six-digit number which the user can change at will.

2.1.1.3 Faculty & staff Banner INB Accounts: Banner INB accounts are established upon written request to Bannerapps@cau.edu. Request must be submitted on the standard Banner User Account Application Form, must specify to which modules or forms access is required, whether access is requested for Query or Maintenance purposes, must have the approval of the department head, and must also have the approval of the Process Owner (Advancement, Financial Aid, Finance, Human Resources, Student, Accounts Receivable) responsible for the security of the forms which access is requested. Login information for Banner INB will be the user's Active Directory credentials (full e-mail address and password).

2.1.1.4 Faculty and Staff UNIX Accounts: UNIX accounts are established upon the written request of a department head. The Username will be the individual's first initial and last name (unless previously assigned at which point an agreed alternative will be designated). A generic password will be assigned and the user will be prompted to change the password upon initially accessing the system. UNIX accounts may be established for temporary employees or contracts/consultants at the written request of a department head, but must specify an end date.

2.2 Individual Responsibilities

2.2.1 All users are required to keep their passwords secure and confidential. In the event of password compromise, the user must immediately change their password.

2.2.2 User passwords shall not be shared with any other individual for any reason. Users may neither ask for nor receive another user's password.

2.2.3 Password must never be written down.

2.2.4 With the exception of multi-use workstations, users must never leave themselves logged into an application or system unlocked and unattended.

2.2.5 All passwords must meet the complexity requirements listed in section 2.3 of this policy.

2.3 Password Complexity Requirements

2.3.1 All passwords must be a minimum length of thirteen characters and meet complex password standards, with the exception of the Banner Web PIN.

2.3.2 The Password cannot contain the user's name or parts of the user's full name that exceed two consecutive characters

2.3.3 Must be at least thirteen characters in length

2.3.4 Must have an uppercase letter

2.3.5 Must have a lowercase letter

2.3.6 Must have a number and/or Special character

2.3.7 Complexity requirements are enforced when passwords are changed or created. With the exception of BannerWeb accounts, passwords will expire every 90 days. Passwords cannot be reused for 720 days.

2.3.8 Passwords will be locked after three unsuccessful logon attempts.

2.3.9 Password reset for PantherIDs can be done by the user by accessing the My Password Portal (Mypassword.cau.edu).

2.4 Lockout Policy

2.4.1 **Lockout Settings:**

2.4.1.1 Account lockout duration of 30 minutes

2.4.1.2 Account lockout threshold after 3 invalid login attempts

2.4.1.3 Reset account lockout counter after 30 minutes of 3rd invalid login attempt

2.4.2 Password resets for Banner and UNIX will require system administrator assistance and can be accessed via the Help Desk (email to support@cau.edu).

2.4.3 Faculty BannerWeb PIN resets must be done by Human Resources.

3.0 Entities Affected by this Policy

All staff, faculty, partners, contractors, consultants, temporary, and other workers at the University and its subsidiaries. The use of the university's network and system resources is a privilege, not a right. This privilege can be revoked or amended when justified. Failure to comply with this policy may result in disciplinary action as outlined in established in the *Clark Atlanta University 2.4.0 Code of Ethical Conduct Policy.*