Policy	User Accounts and Password Policy
Issue	February 1, 2007
Effective	September 1, 2015
Last	August 1, 2015
Responsible Office:	Vice President for Operations and Chief Information Officer/Chief Business Officer
Contact Information:	University Information Technology Services/ Information Security Office Phone: 470-578-6620 Email: iso@kennesaw.edu

1. Purpose Statement

This policy establishes conditions for the use of a Kennesaw State University Access Account and its associated security requirements. These requirements are necessary to help ensure personal privacy and to protect the security of business, research, and academic interactions throughout Kennesaw State University (KSU or the University). Furthermore, this policy informs KSU faculty, staff, and students on the guidelines to protect data integrity and safeguard against security breaches caused by improperly sharing passwords. This policy applies to (but is not limited to) the following KSU Enterprise systems: NetID, OpenLDAP, Active Directory, Banner, and PeopleSoft. It is the responsibility of the individual user to appropriately select and protect his/her passwords.

2. Background

The KSU User Accounts and Password Policy was created to comply with the University System of Georgia (USG) information technology policies. Pursuant to the USG *Information Technology Handbook*, Section 5.1.2, KSU is required to establish and maintain “appropriate internal policies, processes, standards, and procedures for preserving the integrity and security of each automated, paper file, or database.”

3. Scope

The KSU User Accounts and Password Policy applies to all individuals utilizing user accounts to authenticate to University technology resources, including but not limited to students, faculty, staff, external contractors, retirees, and visitors.

4. Exclusions or Exceptions

Where a user account must be accessed in an emergency situation, and only after other options have been explored, the employee's department manager must submit an authorized request through the Information Security Office. The request must include the emergency for which the exception is being requested, the specific business reason, the access duration, and the person to whom temporary access is being requested. Once the purpose or duration has been met (whichever occurs first), the Information Security Office will lock the account until notified in writing by the user assigned to the account.

The vice president for Operations/CIO or his/her designee (controller) retains the final authority to approve or deny the request.

5. Definitions

Definitions are available via the IT Glossary on the KSU Policy Portal at policy.kennesaw.edu.

6. Policy

a. User Account Requirements

1) Each username will be unique to a single individual.
2) Each account is assigned for the sole use of the individual.
3) Username assignment is on a first come, first served basis.
4) All usernames are limited to eight (8) characters or less to accommodate for the maximum username length required by legacy systems.
5) All user accounts will be managed per the KSU User Accounts Standard and Procedure.

b. Password Requirements

1) Birthdates or social security numbers cannot be used as passwords.
2) When a password is reset, it must not duplicate the previous password.
3) In situations where someone requires access to another individual's protected resources, delegation of permissions via technical controls must be used instead of password sharing.
4) Anyone who suspects that their password has been stolen or compromised should change it and contact the KSU Service Desk immediately.
5) All faculty and staff are required to change their password per the schedule defined in the User Accounts and Password Standard and Procedures.

c. Password Security
   1) All passwords are considered sensitive, confidential information and shall not be shared with anyone, including but not limited to administrative assistants, system administrators, and Help Desk personnel.
   2) Passwords stored in clear text is strictly prohibited.
   3) Passwords shall not be written down or stored in an office or publically accessible area.
   4) Passwords shall not be stored in a file on any computer system without encryption.
   5) Passwords shall not be inserted into email messages or other forms of electronic communication.

7. Associated Policies/Regulations

   a. USG *Information Technology Handbook*, 5.1.2 Policy, Standards, Processes, and Procedure Management Standard
   b.

8. Procedures Associated with this Policy

   a. USG Password Authentication Requirement
   b. User Accounts and Passwords Standard and Procedure

9. Forms Associated with this Policy

   a. As required by information in Sections 7 and 8.

10. Violations

Users who are found to be in violation of this policy or any other applicable University policy may be subject to account revocation as well as other disciplinary actions.

11. Review Schedule

The User Accounts and Password Policy is reviewed annually by the Office of the Vice President for Operations/CIO or his/her designee.