USER ACCOUNT AND PASSWORD STANDARD AND PROCEDURE

1. User Account Standards:

Students, Faculty, and Staff:

1.1 A username will be automatically generated based on varying combinations of a person's first initial, last name, and a unique number.

1.2 If a certain combination is found to already exist, then the unique number is incremented until an acceptable username is found.

1.3 Users with a hyphenated last name will have the hyphen removed and the portion of the username that includes the last name will start at the beginning of the last name. Example: Jane Jones-Smith would have the username jjonessm.

1.4 Usernames that do not follow the standard and are already in use will remain available for those individual users.

1.5 Usernames that consist of the first initial, middle initial, last initial, and a unique 4-digit number are no longer created.

Curriculum-Oriented, Contractors, and Non-Standard:

1.6 For Curriculum-Oriented accounts to be used in a teaching environment, the username will end with ".stu".

1.7 For Non-Standard account usernames to be used by people who are not a registered student or employed by Kennesaw State University, the username will consist of the first initial, last name, and a unique number.

Applies to all accounts:

1.8 Each account is assigned for the sole use of the individual.

1.9 In order to ensure accuracy, account names (NetIDs) will not be reused.

1.10 All usernames are limited to eight characters or less to accommodate for the maximum user name length required by legacy systems.

1.11 Special characters are not allowed in usernames.

1.12 Usernames are entered in lower case.

1.13 Username assignment is on a first come, first serve basis

Username Changes:

1.14 Students must wait for a semester break. No exceptions.

1.15 Faculty and Staff should provide an absolute necessity; otherwise wait until a semester break.

1.16 The user assumes full responsibility for informing entities outside the university and any loss of information in the failure to perform this action.

NetIDs for Individuals or Groups other than KSU Students, Faculty or Staff:

The university recognizes that there may be occasions when Network Identification (i.e. NetID, part of KSU's Identity Management System) is required to access electronic services on campus when the individuals or groups needing such access have no permanent or long-term affiliation with the university. The NetID account at Kennesaw State University provides secure access to Web Services like Email, D2L, Lab Resources, Library Services, and Desktop Login. Setup of a NetID account is a pre-requisite to consideration for any Web Service but does not grant access to any service. NetIDs will be provided on a case-by-case basis for these individuals or groups with no fee assessed; however, these individuals or groups must be sponsored by a full-time KSU employee and the sponsorship supported by that employee's Department Head. Furthermore, it must be recognized that there may be charges incurred based on access to specific web services or applications.

A NetID for an individual must be requested on a Service Request form for Long-Term Visitors. For sponsored groups, a NetID Request form for Sponsored Groups must be completed. Both of these forms may be obtained from HR and uses the following form:

https://hr.kennesaw.edu/docs/registered_visitor_job_aid.pdf.

2. User Account Procedures:

Account Creation:

2.1 Undergrad and graduate student accounts are automatically generated at the time the student applies to the institution. These accounts will have an affiliation of “Future Student” until they are accepted. As a “Future Student” they will have

restricted access to services (Email and Banner). Once the person has been accepted to the institution their account affiliation will change to “Student” and all services will be made available at that time.

2.2 Faculty and Staff accounts are created through service usually within 5 business days after being notified of a new employee through the HR department or the Dean of a college. If the account has a start date that is several weeks away, the account will be automatically created 14 days prior to the start date.

2.3 Client machine accounts will be created at first login.

2.4 Lab machine accounts will be created at the time that they are needed. This is required for license specific issues.

2.5 Non-Standard accounts and curriculum-oriented accounts will need to be requested through service at least 48 hours prior to the time that they may be used.

Account Expiration:

2.6 Student accounts will be deactivated 12 consecutive months after they were last enrolled. User data associated with this account (i.e. email) will be deleted 30 days after the account is deactivated.

2.7 Faculty and Staff accounts will be "deactivated" 1 day after the employee leaves or is terminated. User data associated with the account (example: email) will be deleted 30 days after the account is deactivated. Retirees have 30 days to request, through the Service Desk, that their account remain open, otherwise it may be removed.

2.8 Non-Standard accounts will remain for the duration of account request.

Account Locking:

2.9 A student's account can be locked at any time if the user fails to follow applicable KSU Policy & Procedures.

2.10 A faculty or staff account can be locked at any time at the request of their immediate supervisor or if the user fails to follow applicable KSU Policy & Procedures.

2.11 Non-Standard accounts can be locked at any time without explanation.

3. Password Standards:

KSU management and auditors rely on electronic authorizations as part of our internal controls. Internal controls promote efficiency, reduce risk of asset loss, and help ensure the reliability of financial statements and compliance with laws and regulations. Sharing of passwords facilitate fraud and violate State, Board of Regents, and KSU internal

control policies governing such acts of willful and intentional misuse. Passwords and user accounts are given to individuals for individual use to accomplish the mission and business of KSU.

3.1 Per the USG IT Handbook 5.12.3, “All passwords shall be treated as sensitive, confidential information and shall not be shared with anyone including, but not limited to, administrative assistants, system administrators, and helpdesk personnel.”
3.2 Password Complexity:
- 3.2.1 Strong passwords shall be constructed with the following characteristics:
- 3.2.2 Are at least twelve characters in length
- 3.2.3 Must contain the following characteristics:
- 3.2.4 English characters (A-Z, a-z)
- 3.2.5 Numbers (0-9)
- 3.2.6 Non-alpha special character(s).
- 3.2.7 Must not contain the user’s name or part of the user’s name
- 3.2.8 Must not contain easily accessible or guessable personal information about the user or user’s family (such as birthdays, children’s names, addresses etc.)

3.3 Password change frequency:
- 3.3.1 Passwords must be changed at the System-level (e.g., root, Windows Admin, Account Administration) per industry best practices, but not to exceed 365 days.
- 3.3.2 Passwords must be changed at the user-level (e.g., NetID) every 365 days

3.4 Passwords shall not be inserted into email messages or other forms of electronic communication unless encrypted.
3.5 User accounts that have system-level privileges granted through group memberships or programs shall have a unique password from other accounts held by that user.
3.6 Users should not use the "Remember Password" feature of applications. User Should Not Employ Any Automatic Log-In Actions.
3.7 Users should not use the same password for University System of Georgia accounts as for other non-System of Georgia access (e.g., personal ISP account, option trading, benefits, etc.).
3.8 If you suspect your password has been stolen or compromised, change it and contact the KSU Service Desk immediately.
3.9 Birthdays or Social Security numbers must not be used as passwords.
3.10 Passwords may not include common words from an English dictionary or foreign-language dictionary.
3.11 When a password is reset, it must not duplicate the previous password.
3.12 Delegation of permissions via technical controls should be used in situations where someone requires access to another individual’s protected resources.
3.13 Do not leave passwords in a location accessible to others or secured in a location for which protection is less than that required for information that the password protects.
3.14 Use an encrypted connection to avoid sending your password over the network in clear text, which could be viewable by malicious users or programs monitoring the network.
3.15 Most UNIX systems will only use the first eight characters of a password.

3.16 Oracle applications such as LETS only allow $, _, and # as special characters.

Exceptions:

Request any exception to this standard via a service ticket to the KSU Service Desk at https://service.kennesaw.edu

Review Schedule:

The User Accounts and Password and Procedure Standard will be reviewed annually by the Office of the Vice President of Information Technology and Chief Information Officer or his/her designee.

Issue Date	January 1, 2011
Effective Date	February 1, 2018
Last Updated	May 13, 2021
Responsible Office	Office of the Vice President of Information Technology and Chief Information Officer
Contact Information	Office of the Vice President of Information Technology and Chief Information Officer, Office of Cybersecurity Phone: 470-578-6620 Email: ocs@kennesaw.edu