Primary_black

# BOARD POLICIES

|  |  |
| --- | --- |
|  |  |
| DIVISION X Information Technology | ADOPTION DATE 04/2021 |
| POLICY NAME 10.01.07 Account Lifecycle | REVISIONS Revised: |

10.01.07 ACCOUNT LIFECYCLE

**Purpose**

Joliet Junior College (College) utilizes and maintains user accounts including email, network and other applicable accounts for the purpose of conducting business of the College. The purpose of this policy and related procedures is to ensure the proper use of all accounts throughout their entire lifecycle.

Users have the responsibility to use these resources in an efficient, ethical and lawful manner. Use of the College’s accounts evidences the user's agreement to be bound by all JJC Information Technology Division X policies and procedures. In the event a user holds multiple accounts, the most stringent rules of this policy shall apply. This policy and related procedures will govern the lifecycle of applicable accounts.

**Accounts**

The creation, maintenance, and termination of accounts will be governed by institutional procedures.

1. **Employee**: An employee is an individual employed as regular hourly or salaried workers by the College, excluding student employees (student workers). Employee accounts are provided for faculty, staff, and adjunct faculty.
2. **Retiree**: An individual who has officially retired from the College. This category does not include employees who have separated from the College by other means including resignation or termination.
3. **Returning Employee**: If a previous employee returns, efforts will be made to utilize the same account. *Due to account expiration times and possible reutilization of a naming convention, this is not always an option.*
4. **Student Employee (Student Worker)**: Part-time employees who meet eligibility requirements and have been formally placed through the Career Services Department.
5. **Current Student**: Individuals who are not employees of the College who have current class registrations or activity. Student accounts may include dual credit and non-credit students.
6. **Alumni**: Individuals who are graduates or former students of the College.
7. **Guest**: Guests are individuals who are not employees or students but the College has deemed that there is a requirement for the individual to have access to a JJC system. Guest accounts may include but are not limited to vendors, consultants, auditors, lessees, or Trustees.
8. **Service**: Service accounts are a Departmental account but may also include listserv account as approved by the College.
9. **Administrator**: Administrator accounts are separate from the individual’s regular account and are used for tasks that require elevated permissions. These are used in limited situations with approval.
10. **Student Applicants**: Student accounts are created once the student’s application has been processed. Every student will be entitled to one account and email address. If the applicant does not register for a course within a designated time, the account will be deactivated.
11. **Interns**: An internship is a supervised, practical learning experience in the workplace that offers an individual an opportunity to apply, connect, and extend academic theory and operational competencies to build professional skills and networks. This may include internships, externships, and workforce interns. Accounts will be handled according to the institutional procedures related to internship account access.

**User Account Privileges and Responsibilities**

* 1. **Access Privileges/Role Permission** – Accounts will be created with ‘Least Privilege’ which is the standard security advice of granting least privilege, or granting only the permissions required to perform a task. All permission changes need to be approved by the Supervisor. Permission changes for critical roles will be approved by the President or a Cabinet member.
  2. **Authentication** - All employee accounts are required to use Multi-Factor Authentication. If an employee cannot use the provided methods to authentication, they should contact the JJC Information Security Office directly
  3. **Protection of Account Information** Under no circumstances should an account holder share or disclose their login and password to anyone else, including other departmental staff, faculty, students, or any other persons or parties. The Information Technology Department will never ask an account holder for their username and password.
  4. **One Account Per Person** An individual may have multiple accounts of different types, but only a single account of any given type (e.g., a user may have a Mail account and a Windows account, but may not have more than one Mail account).
  5. **Confidential Student Information and Legal Requirements** Any account holder with access to student information will make themselves aware of, and comply with, all State and Federal laws regarding student information (e.g., FERPA).
  6. **Monitoring of Electronic Communication** No user should have any expectation of privacy in any message, file, image, or data created, sent, retrieved, or received by use of the College's equipment and/or access. JJC has the right to monitor any and all aspects of JJC owned computer systems and to do so at any time, without notice, and without the user's permission. The policy applies to all JJC employees, faculty, students, and all other account holders. Examples of when monitoring or review may occur are provided in Institutional Procedure 10.01.06.00.

Accounts for students, staff, and faculty are generated only after all contract, hiring, or admissions paperwork is completed and entered into the system.

Anyone using JJC’s technology resources must comply with JJC’s Acceptable Use Policy and Procedures.