Revision Responsibility: Vice President of Academic Affairs
Responsible Executive Office: Vice President of Academic Affairs

Purpose:

To ensure the security and integrity of both College data and data belonging to individuals, this policy establishes requirements for the digital identification of all users of Platt College computer systems and networks (also referred to as Platt College IT resources). Identified users will securely authenticate to College systems and access only resources that they have been authorized to access.

Policy:

All users of Platt College IT resources will be assigned a unique identity to securely authenticate to College IT resources that they have been authorized to access.

Applicability

This policy covers students, faculty, staff, administration and any and all individuals or entities using any Platt College IT resource and educational delivery format such as face-to-face (eCompanion), blended (eCombination), or online (eCourse).

1. Identification

Management of Identifiers

- **Linked Identifiers.** Platt College maintains dual records identifying all employees, students, and others who use the College’s computing resources. These records correlate Platt College ID and Network ID records.
- **Uniqueness.** Each identifier (College ID) is unique; that is, each identifier is associated with a single person or other entity.
- **One Identifier per Individual.** An individual may have no more than one College ID number and one personal CAMS user name.
- **Non-Reassignment.** Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.
  - Alternative IDs (alternative names registered along with a personal Platt College ID) may be reassigned after a waiting period.
- **Social Security Number.** Social Security Numbers shall not be used to identify Platt College employees or students.

### Platt College Network Identifiers

**Platt College IDs:** consist of alpha-numeric characters and must be three to eight characters in length.

**CAMS IDs:** The CAMS login ID will be the student/faculty/staff first name followed by a period (.) then the last name. In the case of a similar spelling, the last name will be followed by a numeric character starting with 1 and going forward as necessary to accommodate similar name issues. The initial password created by the Platt College CAMS administrator shall be as follows:

- **Student Initial Password = student**
- **Faculty Initial Password = faculty**
- **Staff Initial Password = staff**

Once a new student, faculty, or staff member logs into the CAMS Platt College IT resource the first time s/he will then follow the instructions and change their password.

### Types of Platt College IDs

- **Regular Personal Platt College IDs.** Regular IDs are available to:
  - Authorized, registered students
  - Regular faculty, staff, and administrators
- **Sponsored Personal Platt College IDs.** Sponsored IDs are available to all others subject to the following conditions:
  - The ID is to be used by a specific, named individual
  - The ID is sponsored by a person who has a Platt College ID
  - The sponsor accepts responsibility for ensuring that the sponsored ID is used in support of work consistent with the College’s mission or instruction, research, and community service, and in a manner consistent with the College’s policies.
- **Other Platt College IDs.** IDs are available to identify other kinds of entities such as groups, departments, mailing lists, roles, computer-based services, etc.
Eligibility for Platt College IDs

- **College IDs.** Eligibility begins when the individual accepts the offer of student registration or employment. Eligibility ends when a person’s active association with the College ends (i.e. when an employee is no longer employed or a student is no longer registered). A grace period may be allowed as a courtesy after eligibility ends.

- **Sponsored Platt College IDs.** A sponsored Platt College ID is sponsored for a specific period of time. The sponsor determines the length of sponsorship; sponsorship must be renewed to keep the ID valid. There is no grace period: the entry becomes invalid immediately at the end of the sponsorship period.

- ** Reactivation.** An ID may be reactivated if the individual subsequently rejoins the College, either via regular association or sponsorship.

- **Suspension.** The use of an ID may be revoked if it is used in a manner inconsistent with Platt College policies or if an individual is subject to other administrative action that denies him/her College privileges.

2. Authentication

Access to non-public Platt College IT resources will be achieved by individual and unique logins, and will require authentication, minimally a username and password combination. Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable options exist.

**Authentication Methods**

Authentication methods involve presenting both a public identifier (such as a user name or identification number) and private authentication information such as a personal identification number (PIN), password, token, or information derived from a cryptographic key.

Authentication against Platt College’s central computing infrastructure is recommended when possible. One of the following methods must be implemented:

- Strictly controlled passwords
- Biometric identification
- Tokens in conjunction with a PIN
- Live online proctoring services that replicate the face-to-face proctoring experience over the internet or equivocal virtual testing environment

**No Unencrypted Authentication**
Unencrypted authentication and authorization mechanisms are only as secure as the network they use. Traffic across the network may be monitored, rendering these mechanisms vulnerable to compromise. Therefore, all College services must use only encrypted authentication mechanisms unless otherwise authorized. In particular, historically insecure services, such as Telnet, FTP, SNMP, POP, and IMAP must be replaced by their encrypted equivalents.

**User Responsibilities**

- **Official Actions.** Use of an ID and authentication method to identify oneself to an on-line system constitutes an official identification of the user to the College, in the same way that presenting an ID Card does. Users can be held responsible for all actions taken during authenticated sessions.

- **Integrity.** Regardless of the authentication method used, users must use only the ID and authentication information that they have been authorized to use (i.e. a user must never identify themselves falsely as another person or entity).

- **Confidentiality.** Regardless of the authentication method used, users must keep authentication information confidential (i.e. a user must not knowingly or negligently make it available for use by an unauthorized person).

- **Reporting Problems.** Anyone suspecting that their authentication information was compromised should immediately contact the Coordinator of Online Services.

- **Security Precautions.** Users are encouraged to change their password regularly (at least once every three months), to limit possible abuse of passwords that may have been compromised without the user’s knowledge. Passwords should be chosen so that they are not easily guessable (i.e. not based on the user’s name or birth date).

- **Disciplinary Action.** Individuals who are found to have knowingly violated one of these provisions will be subject to disciplinary action. The possible disciplinary actions for violations, which can include termination of employment or student status, will depend on the facts and circumstances of each use.

3. **Authorization**

Access to information and IT system resources will be granted on a “need to know” or “minimum necessary” basis and must be authorized by the immediate information owner. Any of the following methods are acceptable for providing access:

- **Context-based access.** Access control based on the context of a transaction (as opposed to being based on attributes of the initiator or target). The “external”
factors might include time of day, location of users, strength of user authentication, etc.

- **Role-based access.** Access control model that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Each user is assigned to one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.

- **User-based access.** Security mechanism used to grant users of a system access based upon the identity of the user.

### 4. Identification and Authentication of Local Systems

This section contains recommendations and requirements for systems and services that use local identification and authentication methods rather than centrally supported methods.

- **User IDs.** Systems should use personal IDs to identify their users. This will be less confusing for users, and will ease future transition to centrally supported authentication.

- **Avoid Clear-Text Passwords.** Systems may not transmit reusable passwords across the network unencrypted. Such passwords are vulnerable to capture and abuse.

- **Support Password Quality.** System should check proposed passwords and reject those that are likely to be easily guessable.

### 5. Privacy Statement

Platt College publishes a Privacy Statement which provides detailed information about the use of personal information. By logging into the Platt College Portal to view content or to submit content, students, faculty, staff, and any approved guests agree to abide by the rules and regulations set forth in the Privacy Statement.