2.24 Information Access Security

Last Revised: February 2012

Policy Statement: Piedmont Community College (PCC) is committed to ensuring the security of faculty, staff, and students’ personal information by preventing unauthorized access and establishing user accountability when using IDs and passwords.

Purpose/Definitions: All users must be properly identified and authenticated before being allowed to access secured PCC information assets, except for the general public, who may access the PCC open network with no expectation of security or privacy. This is to provide secure, reliable, and accurate information to authorized users and recipients, and to preserve records integrity.

The College is committed to preventing unauthorized data access through established accountability procedures. Authenticated IDs and passwords are required to access secured PCC information systems. This policy applies to the PCC information users’ community and covers information systems. Examples of information assets include: LANs, workstations, employee and student e-mail accounts, data, and other secured web and server applications.

Student identification in the student e-mail system, once approved, gives current students an e-mail account. Students are also given IDs that will allow access to other teaching related technologies (i.e. student labs or online classes).

Identification and authentication are methods to determine a user’s identity, to verify that it is correct, and to establish accountability. The ability to verify the identity of users is critical for ensuring authorized access to secured system resources and for establishing accountability. Identification distinguishes one user from all others. Authentication is the process of verifying the identity of the user. Besides a human user, any ‘system, application or defined group’ that needs to be authenticated using an ID and password will also be considered as a ‘user’ in this policy.

For purposes of this policy, the following definitions apply:

Access: The ability to make use of any resources of a computer, computer system, or computer network. Examples include the use of these resources to instruct, communicate, input/output, process data.

Authentication: The verification of identifying information of the users (i.e. you are who you say you are).

Authorization: The process of authoring a user access to secured information. Before authorization is approved, authentication must first be verified.

Authorized User: A user who has been authenticated and authorized to use a computer, computer system, or computer network.

Computer: A programmable automated device that performs data processing, telephone
switching, or other arithmetic or logical operations.

**Data Owner:** The appropriate Vice President responsible for a specific type of data.

**Data Custodian:** The President of the College.

**General Public:** Visitors to the PCC campus who by design or by accident access the Internet through access points provided by the College for use by students and employees. General public users have no identification or authentication to use college internal resources and use them with no expectation of security or privacy.

**Identification:** The assignment of a name by which an entity can be referenced; an entity may be high level, such as a human user, or low level, such as a process or communication channel.

**Information Assets:** A definable piece of information, stored in any manner which is recognized as 'valuable' to the College.

**Management Information Systems (MIS) Group:** The technology group which does the work of setting up, modifying, and removing access under the supervision of Data Owners or the Data Custodian.

**Students:** Current or previously enrolled students who have or had information access granted to them as PCC students, including student e-mail accounts and Internet access.

**System:** An assembly of components (hardware, software, procedures, human functions, and other resources) united by some form of regulated interaction to form an organized whole; a group of related processes.

**User/Normal User:** A person, system, application, or defined group that has been authenticated to an IT system and granted access only to those resources to which they have been granted authorization.

**Approval Authority/Monitoring Authority:** Piedmont Community College’s Board of Trustees has approval authority for this policy. The Vice President, Administrative Services has monitoring authority for this policy.

**Procedure:** A supervisor verifies an employee’s identification and recommends authorization by completing a Request for USER ID and Information Assets Access form. The supervisor indicates appropriate access that is needed for job-related duties. MIS will assist supervisors in selecting and developing accesses for users. All authorization requests must be approved by the data owners or data custodian.

The combination of a unique user-ID and a valid password is the minimum requirement for granting access to any secured information assets. A unique user ID must be assigned for each user so that individual accountability can be established for all system activities. MIS will assign
individual user IDs based on system requirements and limitations.

Passwords for all authorizations will consist of a minimum of six characters, two of which are non-alphabetic. Passwords longer than this minimum are acceptable and encouraged. Users must adhere to this standard when changing their passwords. All users are responsible for guarding their passwords to prevent compromise of their authentication tools. Although a co-worker may have adequately provided for security of their password, any unauthorized interception, access, or use thereof by another employee is unethical, a breach of College policy, and a criminal offense under N.C.G.S. 14-458 and the Federal Computer Fraud and Abuse Act.

Authorized users, upon being issued an individual user ID, will sign the Acceptance of USER ID and Information Assets Access form, which will then be filed with their Request for USER ID and Information Assets Access form and maintained by the MIS staff. The Acceptance of USER ID and Information Assets Access form will outline PCC Policy 2.24 - Information Access Security Policy and PCC Policy 2.23 - Acceptable Use Policy.

The MIS staff will use all features available in each system to monitor and control unsuccessful login attempts, to manage passwords to ensure security, and to prevent exploitation of guessed passwords or weaknesses arising from long-life passwords.

Physical access to computer facilities and equipment rooms are limited to MIS staff, maintenance and security personnel, and others who have a legitimate need for access. Physical access is controlled by issued keys and digital locking devices.

PCC will evaluate its business needs and the associated risks for its information systems in conjunction with identification and authentication requirements using appropriate standards and best practices.

It is expected that new systems using IDs and passwords for identification and authentication meet or exceed the basic standards as defined in this policy. Whenever possible, existing systems should conform to this policy. As current systems are upgraded, security access controls using IDs and passwords must also be upgraded to meet or exceed the minimum standards established in this policy and industry practices, whenever possible.

**Legal Citation:** N.C.G.S. 14-458, Federal Computer Fraud and Abuse Act

**History:** Effective October 2001; Revised March 2010, February 2012