2.24 Information Access Security

Last Revised: July 2023

Policy: 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, passwords, and two-factor authentication for network administrators.

Purpose/Definitions:

Purpose

The ability to verify the identity of users is critical for ensuring authorized access to secured system resources and for establishing accountability. As such, the purpose of this policy is to provide secure, reliable, and accurate information to authorized users and recipients, and to preserve record~~s~~ integrity. The College is committed to preventing unauthorized data access through established accountability procedures.

Definitions

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—methods to determine a user's identity, to verify that it is correct, and to establish accountability.

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. 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.

Data Custodian—individuals with day-to-day responsibilities to enter, modify, delete, or disseminate data in their functional area at the direction of the responsible Data Steward. They are accountable for the accurate and timely entry of data assigned to them and can be

responsible for the technical environment and systems supporting the use and security of College Data.

Data Owners—typically senior administrators with specific responsibilities related to compliance and risk with respect to external agencies. Different data owners may have responsibility for different types of data across the College, and act as an authority - judging access in a manner consistent with college policy and rules established by external regulatory bodies - on who is or is not granted access to confidential data and under what conditions.

Data Stewards—individuals who are responsible for overseeing a collection of College Data under the direction of a Data Owner. Data Stewards are responsible for the proper handling and protection of a collection of data. Stewards are responsible for how their data collection is used for the business of the College, interpret their meaning, and produce information out of data.

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

Information Technology Services (ITS)—the acronym used to designate Information Technology Services.

Student—any individual who is or has attended PCC and regarding whom PCC maintains education records.

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.

Two-Factor Authentication (2FA)—a security process that requires a user to provide two different authentication factors to verify their identity before gaining access to a system or service. These two factors typically include something the user knows (such as a password or PIN) and something the user has (such as a security token or mobile device). By requiring two different factors, 2FA adds an extra layer of security and makes it more difficult for unauthorized users to gain access to sensitive information or resources.

User/Normal User—a person, system, application, or defined group that has been authenticated to an ITS 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, Information Technology/Chief Information Officer has monitoring authority for this policy.

Procedure:

Section 1: Authentication

1.1. All users must be properly identified and authenticated before being allowed to access secured PCC information assets.

1.2. This policy applies to all individuals accessing the PCC network resources and data.

Section 2: Process of Verification

2.1. A supervisor verifies an employee's identification and recommends authorization by completing an IT Network Account form.

2.1.1. The supervisor indicates appropriate access that is needed for job-related duties.

2.2. All authorization requests for specific data subsets must be approved by the data owner or appointee and submitted to ITS for implementation.

2.2.1. The data owners will be responsible for reviewing and approving in writing any changes in security settings, access rights, or other configurations.

2.2.2. Data owners will review security access every 6 months for individuals who have access to their area of ownership.

2.3. All users must adhere to PCC policies 2.24 Information Access Security Policy and 2.23 Technology Resources Acceptable Use.

Section 3: Access to Information Systems

3.1. The combination of a unique user-ID, valid password, and utilization of Two-Factor Authentication (2FA) is the minimum requirement for granting access to any secured information assets.

3.2. A unique user ID must be assigned for each user so that individual accountability can be established for all system activities.

3.2.1. ITS will assign individual user IDs based on system requirements and limitations.

3.3. Passwords for all users will consist of a minimum of 12 characters and must be complex.

3.3.1. Passwords longer than this minimum are acceptable and encouraged.

3.3.2. Users are required to change their password every 90 days.

3.3.3. Passwords must never be shared for any reason.

3.4. Any unauthorized interception, access, or use of someone else's credentials by another person 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.

Section 4: Network Security

4.1. ITS 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.

4.2. 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.

4.2.1. Whenever possible, existing systems should conform to this policy.

4.3. 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.

4.4. Physical access to Network Operation Center (NOC) computer facilities and equipment rooms are limited to ITS staff and others who have a legitimate need for access.

4.4.1. Physical access is approved by the CIO and is controlled by issued keys and digital locking devices.

4.5. 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.

Section 5: Student Access

5.1. A completed PCC Application for Admission generates unique usernames and passwords for the prospective curriculum student.

5.1.1. Registration form for continuing education students also generates unique usernames and passwords when the students are entered into Ellucian.

5.2. Students must present valid identification when they first register for classes at the College.

5.2.1. This initial registration activates the usernames and passwords previously assigned to the student.

5.2.2. Once activated, student usernames and passwords provide access to email, student portals, and the learning management system.

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

---

History: Effective October 2001; Revised March 2010, February 2012, August 2021, September 2021, October 2021, May 2022—updated definitions, May 2023, July 2023

Cross-references PCC Policy 2.23 Technology Resources Acceptable Use.