Statement of Confidentiality

Policy 910

1 Introduction

2 Scope

3 Definitions

4 Policy and Procedure Statements

4.1 Statement of Confidentiality

Appalachian State University maintains strict confidentiality requirements and regulations in compliance with the Gramm-Leach-Bliley Act (GLBA), Family Educational Rights and Privacy Act of 1974 as amended (FERPA), and the Health Insurance Portability and Accountability Act (HIPPA) in addition to other federal and state laws. These laws pertain to the security and privacy of all non-public information that may be considered “confidential” or “sensitive” including student information, employee information, and general University information whether it is in hard copy or electronic form.

“Confidential” information is information that either is exempt from disclosure under one of the exceptions to North Carolina's Public Records Act or is prohibited from disclosure by some other applicable statute. Such “confidential” information includes, but is not limited to:

- Personnel file information;
- Student education records (other than directory information);
- Social security or employer taxpayer identification numbers;
- Driver's license, State Identification card, or passport numbers;
- Checking account numbers;
- Savings account numbers;
- Credit card numbers;
- Debit card numbers;
- Personal Identification (PIN) Codes;
- Digital signatures;
- Any other numbers or information that can be used to access a person's financial resources;
- Biometric data;
- Fingerprints;
- Passwords;
- Third-party confidential information or trade secrets.

Disclosure of confidential information is unlawful and against University policies.

“Sensitive” information is information that may be contained in a “public” record within the meaning of the Public Records Act, but that the person or entity who is the subject of the information would likely prefer not be made public unless such disclosure is required by law (e.g., in response to a request for such information under the Public Records Act). It is the policy of Appalachian State University to avoid disclosure of sensitive information except as required by law.

Employees of the University may have access to such confidential or sensitive or privileged information in the course of work activities. Employees of the University understand that they are responsible to use best efforts to protect against unauthorized access to, or disclosure of, such information, and to report any conduct or other facts that might result in unauthorized access to or disclosure of such information. Employees will not release or disclose such information to any unauthorized person, including co-workers who do not have a legitimate business/educational need to know. Any questions regarding the release or disclosure of such information to another person will be directed to the employee's supervisor.

Appalachian State University defines "Unauthorized Access" to be:

1. Access to confidential or sensitive information not necessary to carry out job responsibilities, or for which employees do not have signed authorization.

2. Release of confidential or sensitive information to unauthorized internal or external persons, either in writing or verbally.
3. Release of more confidential or sensitive information to an authorized individual/agency than is essential for meeting the stated purpose of an approved request.
4. Disclosure of system usernames, passwords, or access codes to an unauthorized individual, creating a risk of unauthorized access to confidential or sensitive information.

Confidential or sensitive information may not be divulged, copied, released, sold, loaned, reviewed, altered, or destroyed except as properly authorized within the scope of applicable federal or state laws.

Employees will be held responsible for the misuse or wrongful disclosure of confidential information and/or for failure to safeguard system usernames, passwords, or access codes to confidential information, and are responsible for all activities undertaken using system usernames, passwords, or access codes.

Employees will comply and follow the above guidelines. Failure to do so may subject the employee to loss of access to the University's databases and/or other University systems, and/or may subject them to disciplinary measures as outlined in the University's policies and procedures for performance expectations for faculty and staff which may include suspension or termination of employment. Divulging confidential information to unauthorized persons may make an employee subject to civil or criminal penalties under applicable laws and regulations.

5 Additional References

6 Authority

7 Contact Information

8 Original Effective Date

9 Revision Dates

November 5, 2021 - previously policy 902
July 6, 2023