

WISCONSIN INDIANHEAD TECHNICAL COLLEGE



ADMINISTRATIVE PROCEDURE: G-190 A

TITLE: [Data Security Procedure](#)

CROSS REFERENCE(S):

J-113 (Policy – Privacy of Student Educational Records)

J-115 A (Procedure – Red Flag Rule – Student Identity Theft Prevention)

A. PURPOSE AND APPLICABILITY:

To define the security statement with regard to the processing of requests for the access to the Administrative (Human Resources and Financial) and Student Information Systems (PeopleSoft) and its related employee and student reporting databases and data warehouses.

B. PROCEDURE TO ENSURE DATA IS SECURE

This procedure applies to all WITC faculty, academic staff, classified staff, contract employees, consultants, and student employees who access the PeopleSoft systems in accordance with their work duties at the college. This procedure does not apply to student/employee self-service access to PeopleSoft MyWITC as that access is limited to the student's/employee's own personal record information.

This procedure is associated with policy J-113: Privacy of Student Educational Records (FERPA) as well as procedure J-115 A: Red Flag Rule.

Access to WITC information is provided for personnel when it is necessary in the performance of their duties or in pursuing educational interests. Information is not to be released to others unless they have been approved for access (see policy J-113). In accordance with the Family Educational Rights and Privacy Act (FERPA), student information is confidential and is to be released to other employees only when in the best interests of the student. Confidential information may not be released to third parties.

Information cannot be used for group, club, or personal gain. Students have the option, at the time of registration, to indicate that they wish to have directory information specified as confidential. If information that is supplied to employees contains information about students who have requested confidentiality, the request must be respected and information never released to anyone under any circumstances.

Employee requests for access must be completed on the appropriate forms, and the **Acceptable Internet/Use Agreement** signed by every employee. The agreement addresses "Persons authorized to access WITC's Internet facilities are responsible for maintaining the privacy and security of these facilities, which include electronically stored data and software". Functional module leads approve the authorization of appropriate roles for the employee based on their job duties. Only completed requests will be considered by the PeopleSoft Security Administrator.

Failure to comply with this procedure could result in legal violations of FERPA as well as college policies requiring the control of confidential employee and student information. An individual employee's failure to follow this procedure could result in disciplinary action.

Procedure Adopted: August 3, 2010

PRESIDENT
WISCONSIN INDIANHEAD TECHNICAL COLLEGE