Western Iowa Tech Community College

Information Security Policy Statement

The Information Security Policy Statement was created to comply with the Federal Student Aid requirements for consumer information.

This Policy Statement of Western Iowa Tech Community College (WITCC) views data, third party proprietary information and College information systems as critical business assets. WITCC employees, contractors and agents are responsible for the protection and proper use of College data, third party proprietary information and information systems according to this policy through the provisions set forth below.

1. Restricted College data and third party proprietary information (e.g., licensed software and designated portions of vendor contracts) in the custody of the College staff members and/or faculty shall be used only for official College business and as necessary for the performance of assigned duties. Restricted College data includes student records that are confidential under the Family Educational Rights and Privacy Act (FERPA 1974, as amended), personnel records and other data to which limited access is subject to prior administrative approval.

2. College data or third party proprietary information shall not be altered or changed in any way except as authorized in the appropriate performance of assigned duties.

3. College data or third-party proprietary information shall not be divulged to anyone unless their relationship with the College as an employee, customer, vendor, or contracted temporary employee warrants disclosure and is authorized or required by law and College policy.

4. Unless publicly available, College data shall only be accessed by staff members who are specifically authorized to do so.

5. College information systems shall not be used for personal economic benefit or for political advocacy.

6. Any user IDs and passwords assigned to a staff member shall be used only by that staff member and shall not be divulged to persons not authorized by the College.

7. The College strictly prohibits illegal use of copyrighted software and materials, the storage of such software and materials on College information systems, and the transmission of such software and materials over WITCC network facilities.

8. The College is providing staff members with access to shared resources. Staff members shall not knowingly engage in any activity harmful to the College's information systems, data, or third-party proprietary information. (e.g., creating or propagating viruses, overloading networks with excessive data, instituting or promulgating chain letters, or instigating unauthorized mass postings of any type).

9. WITCC information systems shall not be used to engage in any activity prohibited by College policies, or by state or federal law.

10. College staff members shall not circumvent or subvert any College system or network security measures. They shall not use College email services to harass or intimidate another person. They shall not send email using or impersonating someone else's user ID or password.

11. The College does not routinely inspect, monitor, or disclose electronic mail. However, electronic messages are written records and may be subject to disclosure under the Freedom of Information Act, legal process, or College review upon receipt of a credible allegation of misconduct. The College will investigate and may pursue appropriate internal or external civil or criminal proceedings when misuse of College data, third party proprietary information, or College computing resources is suspected.

12. Failure to comply with any of the above stated policies may result in a staff member being disciplined or terminated from his or her position, in accordance with general employment policies and procedures that apply to respective categories of employees.

Information Security – Safeguarding Customer Information

This section addresses the requirements established by the Federal Trade Commission (FTC) for postsecondary educational institutions participating in the Federal Student Aid (FSA) programs.

All customer information and data of any type at WITCC is safeguarded through technological methods, security assessments, testing and policies regarding the appropriate use of all data and private information. The office of the Dean of IT is responsible for directing this compliance. These methods insure that the safeguards in place provide the desired level of protection and confidentiality to all College information is provided. The College System Administrators and Networking staff are assigned the duty to maintain the approved access controls and security.

The college IT department continually monitors and adjusts security measures to protect against changing security threats as well as in response to attacks to the system. Automated notifications are in place to inform the IT staff of potential threats allowing for preventative countermeasures.

The IT department works with all vendors to make certain they understand the requirements to security and confidentiality and only allows access to data when absolutely necessary. The activity in these instances is monitored by qualified IT personnel the entire time this access is active. All administrator accounts assigned to vendors are disabled when not in approved use. All College IT Administrator accounts are to be used for system work only and never to be used for typical user related activities or allowed to access the Internet.