# Privacy Policy

## 1.0 Purpose

Jefferson State Community College is committed to protecting your privacy and making it easier and more efficient for individuals and businesses to interact with the College. It is critical for individuals and businesses to be confident that their privacy is protected when visiting Jefferson State Community College campuses and websites.

## 2.0 Scope

The Privacy Policy applies to all individuals who access the campus computer systems, websites and networks.

## 3.0 Policy

Jefferson State Community College does not collect any personal information unless it is provided voluntarily by sending an e-mail, completing a request form or application, accessing online services, or interacting in distance education courses. When visiting Jeffersonstate.edu, the College may automatically collect and store the following information about your visit:

- The Internet Protocol address of the computer that accessed the site
- The type of browser, its version and the operating system on which that browser is running • The web page from which the user accessed the current web page
- The date and time of the user's request
- The pages that were visited and the amount of time spent on each page

The information automatically collected is used to improve the College's website content and to help administrators understand how users are interacting with its

websites. This information is collected for statistical analysis and to determine what information is of most and least interest to our users.

The information collected on the College's websites is not collected for commercial marketing purposes and the College is not authorized to sell, or otherwise disclose, the information collected for commercial marketing purposes.

Jefferson Community College may collect or disclose personal information without consent if the collection or disclosure is:

- made pursuant to a court order or by law
- for the purpose of validating the identity of the user
- information to be used solely for statistical purposes that is in a form that cannot be used to identify any particular person

Jefferson State Community College may disclose personal information to federal or state law enforcement authorities to enforce its rights against unauthorized or attempted unauthorized access to college information technology assets.

Information that is collected via Jefferson State Community College systems from the user will not be used for any other purpose than what it was intended for, except for the exceptions stated above.

Among the laws and regulations that mandate baseline privacy and information security controls, the most notable for the College include the following:

**Health Insurance Portability and Accountability Act (HIPAA)** - Protective Health Information (PHI) may be used and disclosed for Treatment, Payment, and Healthcare Operations (TPO). The information that is disclosed must meet the "Minimum Necessary" standard. This means the least information required to accomplish the intended purpose.

**Family Educational Rights and Privacy Act (FERPA)** - Protects the privacy of student education records and gives parents certain rights with respect to their children's education records.

In addition to the Jefferson State Community College Catalog and Handbook, the following yearly FERPA notification is supported by the College's IT and is provided for all students.

Additional student privacy information, may be found on the Family Policy Compliance Office website by following this link: http://familypolicy.ed.gov/

**Payment Card Industry (PCI) Data Security Standards** – A framework of standards and compliance requirements designed to protect consumer payment card data. Jefferson State Community College supported information systems do not store credit card data. The College utilizes TouchNet to interface with the Banner ERP/SiS for payments. The data is scanned and transmitted real-time and no data is stored in any College information system.

Additional laws and regulations apply in the wake of unauthorized disclosure of individuals' data, requiring the College's IT to take specific actions if any protected data may have been disclosed either accidentally or maliciously to unauthorized parties. Individuals who handle protected data are encouraged to speak with their managers to better familiarize themselves with relevant laws and regulations.

**Gramm-Leach-Bliley Act** - The GLB Act, or GLBA, is also known as the Financial Modernization Act of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. To be GLBA compliant, financial institutions must communicate to their customers how they share the customers' sensitive data, inform customers of their right to opt-out if they prefer that their personal data not be shared with third parties, and apply specific protections to customers' private data in accordance with a written information security plan created by the institution.

The primary data protection implications of the GLBA are outlined in its Safeguards Rule, with additional privacy and security requirements issued by the FTC's Privacy of Consumer Financial Information Rule (Privacy Rule), created under the GLBA to drive implementation of GLBA requirements. The GLBA is enforced by the FTC, the federal banking agencies, and other federal regulatory authorities, as well as state insurance oversight agencies.

## 4.0 Enforcement

Any employee found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment.

## 5.0 Disclaimer

The information provided in this privacy policy should not be construed as giving business, legal or other advice, or warranting as fail proof regarding the security of information provided through Jefferson State Community College systems.

## 6.0 Revision History