THREE RIVERS COLLEGE
INFORMATION TECHNOLOGY POLICY

Section: 8000 Information Technology	
Sub Section: 8200 Data Governance	
Title: ITP 8201 Data Security	Page 1 of 3
Associated Regulation: ITR 8100 Acceptable Use	
Associated Policies: ITP 8100 Acceptable Use; ITP 8202 Electronic Communication; ITP 8203 Disaster Recovery	
References: Computer Services Electronic Data Governance Operating Manual	
Supersedes: NA	
Responsible Administrator: Chief Technology Officer	
Initial Approval: 06-21-2017	Last Revision: 04-19-2023

Three Rivers College is committed to ensuring that all access to and uses of sensitive information are performed in a secure manner. Therefore, measures are in place to minimize the risk to the College from unauthorized disclosure of sensitive data, whether accidental or deliberate. To comply with data protection guidelines, sensitive information must be collected and used appropriately, stored safely, and not disclosed to any other person(s) unlawfully.

The purpose of this Data Security Policy is to define the security controls necessary to safeguard the confidentiality and integrity of sensitive College information. This policy provides a framework in which security threats to College information systems can be identified and managed on a risk basis and establishes terms of reference which ensure uniform implementation of data security controls throughout the college.

The United States follows what is referred to as a 'sectoral' approach to data protection legislation. Under this approach, laws of data protection and privacy rely on a combination of legislation, regulation, and self-regulation rather than governmental control. Therefore, the College establishes self-regulated guidelines for data security.

Accurate, timely, relevant, and properly protected information is a critical asset of Three Rivers College. The College recognizes that failure to implement adequate security controls over sensitive information could potentially lead to:

- Irretrievable loss of important data.
- Serious financial consequences.
- Damage to the reputation of the college; and
- Legal penalties.

THREE RIVERS COLLEGE
INFORMATION TECHNOLOGY POLICY

Section: 8000 Information Technology	
Sub Section: 8200 Data Governance	
Title: ITP 8201 Data Security	Page 2 of 3
Associated Regulation: ITR 8100 Acceptable Use	
Associated Policies: ITP 8100 Acceptable Use; ITP 8202 Electronic Communication; ITP 8203 Disaster Recovery	
References: Computer Services Electronic Data Governance Operating Manual	
Supersedes: NA	
Responsible Administrator: Chief Technology Officer	
Initial Approval: 06-21-2017	Last Revision: 04-19-2023

The Network Administrator performs the duties of the Data Security Officer (DSO) for the College. The DSO shall direct a Data Security Team (DST) which consists of the system administrator, Chief Technology Officer (CTO), and assigned data stewards. The Data Security Officer in conjunction with the Data Security Team, shall be responsible for:

- Establishing, maintaining, and enforcing electronic and physical information security and access standards for all entities under the direction of the College President.
- Enforcing board-approved technology policies and regulations established collaboratively by the CTO and the College Cabinet.
- Managing information security incidents, including establishing and communicating incident response procedures for all members of the campus community.
- Adopting and implementing industry best practices and standards for secure transportation and transmission of electronic data.
- Informing all college information systems users of their individual responsibilities, and establishing standards to protect sensitive data and privacy.
- Working in conjunction with the College Cabinet and their associated areas of responsibility to protect the security of electronically held information.
- Periodically auditing college-controlled information systems for vulnerabilities.

This Data Security Policy applies to anyone authorized to access college data. Failure to comply with this policy may result in loss of data access privileges and possible disciplinary action.

Section: 8000 Information Technology	
Sub Section: 8200 Data Governance	
Title: ITP 8201 Data Security	Page 3 of 3
Associated Regulation: ITR 8100 Acceptable Use	
Associated Policies: ITP 8100 Acceptable Use; ITP 8202 Electronic Communication; ITP 8203 Disaster Recovery	
References: Computer Services Electronic Data Governance Operating Manual	
Supersedes: NA	
Responsible Administrator: Chief Technology Officer	
Initial Approval: 06-21-2017	Last Revision: 04-19-2023

DOCUMENT HISTORY:

06-21-2017:   Initial approval of policy ITP 8201 Data Security.

04-19-2023:   Changed DSO to Network Administrator from Chief Technology Officer.