SECTION 3 – GLBA GENERAL CONTROLS

3.1 - ACCESS CONTROL

Access, Security and Control of Data and Information Policy

Introduction

This policy establishes a standard for the protection of the college computer information systems, data, and software. This policy establishes rights and responsibilities for the protection of staff and faculty who use these systems.

Policy

Data contained in the college systems are the property of West Virginia University at Parkersburg and represent official college records. Users who accept access to this data also accept responsibility for adhering to certain principles in the use and protection of that data.

- Information systems within the college shall be used only for and contain only data necessary for fulfillment of the college's mission.
- College data shall only be used for the legitimate business of the college.
- Due care shall be exercised to protect college data and information systems from unauthorized use, disclosure, alteration or destruction.
- College data, regardless of who collects or maintains it, shall be shared among those faculty or staff whose responsibilities require knowledge and access of such data.
- Applicable state and federal laws, as well as college policies and procedures concerning storage, retention, use, release, transportation, and destruction of data and/or all information systems contents and components shall be observed.
- Appropriate college procedures shall be followed in reporting any breach of security or compromise of safeguards.
- College information systems shall be implemented in such a way that:
    - Accuracy and completeness of all system contents are maintained during storage and processing.
    - Data, text and software stored and processed can be traced forward and backward for audit capability.
    - Information systems capabilities can be re-established within an acceptable amount of time upon loss or damage by accident, malfunction, breach of security or act of God.
    - Actual or attempted security breaches can be detected promptly.

- Any employee engaging in unauthorized use, disclosure, alteration, or destruction of information systems or data in violation of this policy shall be subject to the appropriate disciplinary action, including possible dismissal.
- Users may not utilize information systems to access data that they have not been given explicit access to. This data can include, but is not limited to:
    - transcripts, grade reports, enrollment reports
    - financial aid information
    - personnel, leave, salary reports
    - reports for government or funding agencies
    - fund-raising activities
    - mailing lists and labels
    - private or public release of data to outside parties such as students, parents and news media.

Responsibilities

The proper safeguarding of college information systems and the data contained wherein shall be the responsibility of all faculty and staff that have access and knowledge of the system or data. Specific responsibilities are as follows:

- Data Management - for each source of data, a designated manager is responsible for permitting any requested access to ensure appropriate permissions are granted.
- Management - all levels of management are responsible for ensuring that system users within their area of accountability are aware of their responsibilities as defined within the policy. Specifically, managers are required to validate the access requirements of their staff according to job functions, prior to submitting requests for the provisions of access, and for ensuring a secure office environment with regard to college information systems.
- Users - users are responsible for the protection, privacy, and control of all data, regardless of the storage medium. Users must ensure that data, including media, are maintained and disposed of in a secure manner. Users are responsible for understanding the meaning and purpose of the data to which they have access, and may use this data only to support the normal functions of the user's duties. Users are responsible for all transactions occurring under their account credentials. Account credentials shall not be shared with anyone else under any circumstances unless the Chief Information Officer specifically approves an exception.
- Chief Information Officer - Responsible for ensuring that appropriate security controls are being provided, including protection of all areas from risk of exposure.
- Office of Information Technology staff - responsible for providing administrative, technical and educational support in the area of information security for all users of administrative systems. This support includes, but is not limited to:

- creation and deletion of user accounts, after appropriate approval has been obtained.
- providing access to administrative systems, transaction, or production after appropriate approval.
- Recommendations to the Chief Information Officer on appropriate training to ensure consistent practice among departmental support personnel.

Violations

The Chief Information Officer is the policy administrator for information technology resources and will ensure that this process is followed. Additionally, deans, directors, and department heads are responsible for compliance with college policy within their respective administrative areas.