**INFORMATION PROTECTION**

## 1.0 PURPOSE

All employees of Wheeling Jesuit University are responsible for protecting information from unintended or unauthorized disclosure to either internal or external sources. Furthermore, Wheeling Jesuit University respects the information associated with the business practices of other institutions and organizations. Consequently, the acquisition or collection of information is also regulated and employees will be held to the same standards in obtaining another institution or organization's information.

## 2.0 POLICY STATEMENT

2.1 Definitions

a. "Information" includes printed or electronic files, emails and verbal communications.
b. "Protection" refers to the level of security for the information from inception through disposal to include retention, storage and transfer.
c. "Hierarchy of Security" refers to the level of protection applied to the information.
d. "Sharing" means conveyance of information to include transmission via copying, mailing, electronic transfer or speech. This also includes receipt of information, the acquisition of which could adversely affect the university's reputation.
e. "Nondisclosure Agreement", or NDA, is a legal instrument designed to protect information deemed "Restricted" by the university.

2.2 Coverage

Information that is to be protected includes data specific to Wheeling Jesuit University and data obtained from or supplied to a third party. Supervisors, directors and administrators are to apply the appropriate level of security associated with the information that they manage and share. Secretaries, administrative assistants, staff employees and student workers are to respect the security associated with information and understand that they are functioning as an extension of their supervisors; they are bound by the same security as the supervisor to whom they are assigned.

2.3 Hierarchy of Security

a. Public: Information of general knowledge that can be shared freely among the public or employees of the university. Examples would include: university calendars, brochures, mission statements, etc.
b. Private / Confidential: Information pertaining to specific individuals or departments that is controlled by necessity or regulation. Examples would include: individual personnel files, student files / academic records, financial data pertaining to a department within the university, technology, funding, etc. This information is protected on a "needs to know" basis among management and administration and can only be shared at that level or above.
c. Restricted: Information that is protected, the dissemination of which could damage either the university or individuals within the university. Examples would include: undisclosed, non-public, university financial data, information of a strategic or proprietary nature, intellectual capital, technology and research impacting a program or the potential start-up of an entrepreneurial outgrowth, etc. This information is protected on an "eyes only" basis among administrators and can only be shared at that level or above. If it is appropriate for an employee outside of administration to handle restricted information, that employee shall be preapproved by the President and sign an NDA beforehand.

2.4 Identifying / Handling Information

a. Information that is jointly shared among management and administration shall be considered “Private / Confidential.” Other employees who, in the course of their employment, handle such information for a supervisor shall consider it “private / confidential”.
b. All information that is “Restricted” shall be identified at the time of development or dissemination.
c. The university will employ legal and ethical means to collect or disseminate information and will not collect or disseminate information unless the party from whom the information is obtained or to whom the information is sent is agreeable to the university’s application of that information.
d. Employees should avoid: sharing or unauthorized discussion of private / confidential and restricted information with friends, family or student workers in casual conversation or holding authorized discussions in public venues; leaving private / confidential or restricted information lying openly on desks, computer screens or copiers; printing on remote printers and not accessing the information immediately afterward; downloading information to personal devices; sharing, disseminating or discussing information with outside individuals absent the university’s consent.

2.5 Consequences for Failure to Adhere

Individuals who fail to adhere to this policy may be disciplined. Such discipline may range from a simple memo or counseling session wherein the employee is informed of individual obligations under this policy through corrective discipline up to and including termination. The level of discipline will be determined by prior occurrences, hierarchy of information shared, intent of the party and exposure to the university.