WAGNER COLLEGE
INFORMATION TECHNOLOGY

Data Security and Stewardship Policy

Wagner College takes seriously the proper use and protection of personal and institutional data. This policy pertains to all individuals who are involved in Wagner College business, whether they are paid or volunteers. Department heads are responsible for functioning as data stewards, ensuring that all individuals in the department are familiar with their responsibilities under this policy. The Provost will function as the department head for all academic departments.

All individuals involved in College business (full- and part-time employees, student workers, volunteers) are required to sign the Wagner College Confidentiality Agreement. Full- and part-time employees sign the agreement at hire and the agreement is kept on file in Human Resources. Students and volunteers sign the agreement when they start working for a College department and the department keeps the agreement on file.

I. Data Sources and Types

The majority of College data are maintained within our administrative system (i.e., Jenzabar) and accessed either directly through the database interface or through a website (e.g., myWagner, Moodle). Often, data are transferred into a spreadsheet for further manipulation and sharing. Data may be collected on forms (electronic or paper) and stored within email accounts, in file cabinets, or on a workstation or server. Regardless of the way that the data are obtained and stored, all College data must be maintained in a secure manner.

College data fall into two main types: personal information and institutional information. Personal information includes, but is not limited to, social security and ID number, financial information, grades, and health records. Directory information (e.g., home address, telephone number, email address) is not confidential, unless an individual has asked that it be kept confidential. Institutional information includes, but is not limited to, College finances, personnel records and teaching evaluations.

II. Social Security Number

Federal and state law requires the collection of social security number (SSN) for certain purposes. However, widespread use of a person's SSN is a major privacy concern. With incidents of identity theft increasing, the protection of everyone's personal identity is important and steps are taken to protect everyone's information.

It is Wagner College policy that any report, web page or data extract will NOT contain SSNs unless required by law or by prior approval of senior management of Wagner College. This includes those specialized reports that contain parts of the SSN.

By law, Wagner College must collect and maintain SSNs for reporting and communicating to various legitimate agencies. It is therefore imperative that each person's SSN is recorded accurately within the database.

III. Permissions

Each College office and the personnel within that office have access to only those data they need to efficiently conduct College business. An individual may only access, manipulate or change data as required to fulfill their assigned duties. Level of data access is controlled through permissions assigned in the administrative system and to department folders on the server. Permissions are granted to individuals when a formal request is made (via email) to Information Technology by the department head or vice president.

Individuals are not allowed to circumvent the level of data access given to another individual by providing them access to data that they could not view themselves.

IV. Passwords

It is recommended that passwords used for College business remain separate and different from any personal passwords an employee might have. In the event a password is compromised, damage is mitigated by constructing these passwords differently. All employees are required to have strong passwords, which have the following characteristics:

- Both upper and lower case characters (a-z, A-Z)
- Contain special characters and numbers (0-9, !@#$%^&*()_+{}|":<>?/.,;'[]\)
- Are at least 8 characters in length, 10 or more characters recommended
- Cannot be found in a dictionary
- Are not based on names or other personal information

a. *Password Protection*

To keep individual passwords safe and secure, all employees should adhere to the following guidelines:

- Employees should not reveal their passwords to a co-worker
- Employees should not discuss the format or complexity of their passwords
- Employees should not write down or store their passwords in visible or easily accessible locations

- Employees should NEVER send their passwords in an email message
- Employees should NEVER speak their passwords over the phone
- Employees should NEVER reveal their passwords to ANYONE

Please be advised that Information Technology employees will NEVER ask for passwords in any form - via email, phone, or in person. In the event an employee receives a request to reveal a password, s/he should report the incident to the Chief Information Officer immediately.

V. Securing Data: On-Campus

Individuals must be cognizant of maintaining the security of all College data. This includes both hard copies and digital copies of data.

a. *Hard copies*

Hard copies must be properly stored within department offices, in locked file cabinets whenever possible, and these offices must be locked when they are not occupied. Any piece of paper that includes these data must be shredded prior to disposal.

b. *Digital copies*

Whenever possible, College data should be maintained on a College server. This would mean the data are kept within the administrative system or within a department network folder. Securing these data require that every individual completely logs off of the administrative system and the network before leaving their computer unattended.

At times, individuals may move data from the network and onto the hard drive of their workstation. These instances should be for very limited time frames and the data should be returned to the network and deleted from the hard drive before the computer is left unattended. Data left on the hard drive of the workstation is accessible to anyone who can gain access to the workstation, no permissions required.

c. *Sharing data*

Data files are often shared among individuals within the same office and across offices. Within an office, the department network folder is the most secure way in which to share files. A network folder is also the most secure way to share data across offices. A project-based network folder can be created and appropriate permissions assigned. A Moodle course could also be created for a project.

Small amounts of data may also be transferred between offices via email, on a CD or on a thumb drive. Non-password protected emails may contain Wagner College ID numbers, but must never

contain a social security number. Files should be password-protected before sent via email. The password should be sent in a separate email. Both parties should be sure to completely delete the message from their Inbox, Sent and Trash folders once they have transferred the data. Data files stored on CDs and thumb drives should be deleted after the transfer. CDs must be destroyed prior to disposal.

VI. Securing Data: Off-Campus

Accessing data while off-campus requires even greater diligence than when on-campus. Department heads must ensure that any employee given the ability to do so must be aware of the vulnerability that the College may suffer if these data are lost while not on campus property.

If an employee does lose data while off-campus (laptop or file folder is stolen/missing) s/he must notify her/his supervisor immediately. The supervisor must then notify their Vice President and the Chief Information Officer.

a. *Hard copies*

There should be few instances when an individual leaves campus with a hard copy of College data. The individual who does so must maintain the absolute security of that copy and ensure that it is shredded upon disposal.

b. *Digital copies*

All individuals have remote access to their network folders, including department folders. Any individual who configures a computer not owned by Wagner College to remotely access their folders must never move data from the folder to the hard drive of that non-Wagner computer.

Remote access to the administrative server is available through a virtual private network. This network will only be configured on a Wagner-owned laptop and permission must be granted by the appropriate Vice President. Individuals connecting to the administrative system while off-campus must exert the highest level of caution. All individuals who are given access to the virtual private network must also have the hard drive of their laptop encrypted.

Individuals who access their network folders from a College-owned laptop must be sure that they keep all of the data on the network and do not save any data onto the laptop hard drive. Any individual who has the need to carry College data on the hard drive of their laptop must have the hard drive encrypted and use the e-token system, even if they are not using the virtual private network.