Confidentiality and Information Security Agreement

Willamette University regards security and confidentiality of data and information to be of utmost importance. Further, it is the intent of this policy to ensure that confidential information, in any format, is not divulged outside of Willamette University without explicit approval to do so by the President of the University, or other duly authorized executives of the University. The University requires all users of data and information to follow the procedures outlined below:

Confidentiality of Information Including Data

Each individual granted access to data, verbal or written information, and hard copy information that is generally viewed or officially deemed "confidential" holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Users or receivers of University data and information are required to abide by all applicable Federal and State guidelines and University policies regarding confidentiality of data, including, but not limited to the Family Education Rights and Privacy Act (FERPA); the Gramm-Leach-Bliley Act (GLB); The Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Fair Credit Reporting Act (FCRA) . Personnel records and information also holds special status as confidential information. All users of University data and information must read and understand how these laws and any policies that reference them apply to their respective job functions. All users with access to Datatel or other university computer systems acknowledge that they have read and agree to abide by the University's Acceptable Use Policy found at www.willamette.edu/wu/policy/network.htm.

Data/Information Systems

Any individual with authorized access to Willamette University's computer information system, records or files is given access to use the University's data or files solely for the business of the University and must not divulge this information outside of The University except for approved University business requirements approved by the President of the University such as procurement of insurance and financial/banking requirements. Specifically, with respect to University records or information, individuals must:

1. Access data solely in order to perform his/her job responsibilities.
2. Not seek personal benefit or permit others to benefit personally from any data that has come to them throughout their work assignments.
3. Not make or permit unauthorized use of any information in the University's information system or records.
4. Not enter, change, delete or add data to any information system or files outside of the scope of their job responsibilities.
5. Not include or cause to be included in any record or report, a false, inaccurate or misleading entry known to the user as such.
6. Not alter or delete or cause to be altered/deleted from any records, report or system, a true and correct entry.
7. Not release University data other than what is required in completion of job responsibilities.
8. Not exhibit or divulge the contents of any record, file or information system to any person unless it is necessary for the completion of their job responsibilities.

It is the individual's responsibility to report immediately to his/her supervisor any violation of this policy or any other action, which violates confidentiality of data.

Verbal and Written Information

As with stored information above, information received verbally or in writing may also be limited in disclosure. This includes, but is not limited to, the following specific types of information:

1. Employee personnel records and verbally shared information.
2. Student records and verbally shared information.
3. Health records and verbally shared health information of students and employees.

Security Measures and Procedures

All users of University information systems are supplied with an individual user account to access the data necessary for the completion of their job responsibilities. Users of the University information systems are required to follow the procedures outlined below:

1. All transactions, processed by a user ID and password, are the responsibility of the person to whom the user ID was assigned. The user's ID and password must remain confidential and must not be shared with anyone.

- Using someone else's password is a violation of policy, no matter how it was obtained.
- Your password provides access to information that has been granted specifically to you. To reduce the risk of shared passwords – remember not to post your password on or near your workstation or share your password with anyone.
- It is your responsibility to change your password immediately if you believe someone else has obtained it.

2. Access to any student or employee information (in any format) is to be determined based on specific job requirements. The appropriate Department Chair, Department Director/Manager, Dean, and/or Vice President is responsible for ensuring that access is granted only to authorized individuals, based on their job responsibilities. Written authorization must be received by WITS prior to granting system access.

You are prohibited from viewing or accessing additional information (in any format) unless you have been authorized to do so. Any access obtained without authorization is considered unauthorized access. In order to prevent unauthorized use, the user shall log off of all applications that are sensitive in nature, such as employee/student personal information, when leaving their workstation. An alternative is to establish a workstation password or lock your session. This is especially important during breaks, lunch and at the end of the workday. If you require assistance in establishing or revising your workstation password, please contact the WITS help desk.

3. Passwords should be changed periodically and/or if there is reason to believe they have been compromised or revealed inadvertently.

4. Upon termination or transfer of an employee, Human Resources will notify WITS.

5. Disclosure of any information deemed "confidential" should be limited based on operational "need to know". External inquiries by the media or other outside agencies should be managed according to specific policies pertaining to the same. Before disclosure, consulting with the appropriate internal authority is required (ie. Human Resources relative to employee information; Registrar related to student information; Student Health Center Director related to student medical information; Marketing relative to any media inquiry.)

6. Generally, students and temporary employees should be limited in access to the University record system. Approval by the Department Chair, Department Director/Manager, Dean, and/or Vice President in charge of the respective area is required if it is determined that access is required. The student or temporary employee is to be held to the same standards as all University employees, and must be made aware of their responsibilities to protect student and employee privacy rights and data integrity, including signing of this agreement.

Written authorization must be received by WITS prior to granting system access.

AGREEMENT

I agree to properly secure and dispose of confidential information in a manner that fully protects the confidentiality of records. I also understand that my access to University data and information systems is for the sole purpose of carrying out my job responsibilities and confidential information is not to be divulged outside of the University, except as identified herein. Breach of confidentiality, including aiding, abetting, or acting in conspiracy with any other person to violate any part of this policy, may result in sanctions, civil or criminal prosecution and penalties, employment and/or University disciplinary action, and could lead to dismissal, suspension or revocation of all access privileges. I understand that misuse of University data and information and any violation of this agreement, or policies related to FERPA, HIPAA or GLB, are grounds for disciplinary action, up to and including dismissal. This agreement shall not abridge nor supersede any rights afforded faculty members under the Faculty Handbook, or other policies or contracts.

I have read and agree to comply with the Willamette University Confidentiality Agreement.

_____	_____	_____	
Individual's Name (Please Print)	Department	Signature	Date