University of Portland

INFORMATION SECURITY POLICY

1. **PURPOSE:** This policy ensures that the confidentiality, integrity, and availability of each piece of information owned or entrusted to the University of Portland is protected in a manner that is consistent with the value attributed to it by the University, the risk the University, applicable laws, and the nature of information.

2. **SCOPE:** This policy defines the principles to which students, faculty, staff, and the University community must adhere to when handling information owned by or entrusted to the University of Portland in any form.

   a. **Summary of Principles:**

   - Defining the confidentiality, integrity and availability requirements for information used to support the University's objectives,
   - Ensuring that those requirements are effectively communicated to individuals who encounter such information, and
   - Using, managing and distributing such information — in any form, electronic or physical — in a manner that is consistent with those requirements.

   b. **Relationship to Other Policies:** The University has other policies that may apply to the handling of specific information in specific instances. When a more specific policy applies, it should be followed.

   c. **Relationship to Laws:** A number of laws address how some information must be handled (see Appendix A). The University's policy is to follow all laws that govern the use of information.

3. **POLICY:** While much of this policy document focuses on our legal obligations and the process of determining and communicating the sensitivity of information owned by or entrusted to the University, it also contains a number of requirements to which anyone who handles such information must adhere.

   a. **Responsibilities:** Faculty, staff and student employees are responsible for their use of Level 1 and Level 2 information and must adhere to the following:

   - Must not in any way divulge, copy, release, sell, lend, review, alter or destroy any Level 1 or Level 2 information except as necessary within the scope of their professional activities.
   - Must take appropriate measures to protect Level 1 and Level 2 information wherever it is located, e.g., held on physical documents, stored on computer media, communicated over voice or data networks, ex- changed in conversation.
   - Must safeguard any physical key, ID card or computer/network account that allows them to access level 1 information. This includes creating computer passwords that are difficult to guess and that conform to the University's Password Policy.
   - Must render unusable Level 1 information held on any physical document or computer storage medium (e.g., diskette, CD, magnetic tape, hard disk) that is being discarded.
   - Must report any activities that they suspect may compromise Level 1 or Level 2 information to their immediate supervisor and the Vice President for University Operations.

   b. **Accountability:** All information gathered and maintained by employees of the University of Portland for the purpose of conducting University business is considered institutional information and thus each individual who uses, stores, processes, transfers, and/or maintains this information is responsible and held accountable for its

appropriate use.

c. **Information Collections and the Responsibilities of Information Custodians:** University-maintained information must be protected against unauthorized exposure, tampering, loss and destruction, wherever it is found, in a manner that is consistent with applicable federal and state laws (see **Appendix A)** with the information's significance to the University as described in this policy, and with the nature of the information. Achieving this objective requires that University information be segregated into logical collections (e.g., medical records, employee benefit data, payroll data, undergraduate student records, graduate student records, personal data regarding alumni friends and benefactors, financial records), and that each collection be associated with an individual known as an "Information Custodian" who must:

- Define the collection's requirements for confidentiality, integrity and availability (see ***Data Risk Classification Guidelines*** for requirement classifications),
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection,
- Work with Deans, Chairs, and Department Heads to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information) and to convey the collection's requirements to any person authorized to access the information.

The custodian of a logical information collection is typically the head of the department on whose behalf the information is collected or that is most closely associated with the information. A list of Information Custodians may be found in **Appendix B**.

d. **Responsibilities of Deans, Chairs, and Department Heads:** Deans, Chairs, and Department Heads are required to:

- Understand the security-related requirements for the information collections used within their respective departments by working with the appropriate Information Custodians and their designates.
- Develop procedures that support the objectives of confidentiality, integrity and availability defined by the Information Custodians or designates and ensure that those procedures are followed.
- Effectively communicate any restrictions to those who use, administer, process, store or transfer the information in any form, physical or electronic.
- Ensure that each staff member understands his or her information security-related responsibilities and acknowledges that he or she understands and intends to comply with those requirements by having them review the ***Data Risk Classification Guidelines*** and reading this policy.
- Report to the Vice President for University Operations any evidence that information has been compromised or any suspicious activity that could potentially expose, corrupt or destroy information.

e. **User Responsibilities - Protecting Information Wherever It Is Located:** Each individual who has access to information owned by or entrusted to the University is expected to know and understand its security requirements and to take measures to protect the information in a manner that is consistent with the requirements defined by its Information Custodian, wherever the information is located, e.g.:

- On printed media (e.g., forms, reports, microfilm, microfiche, books)
- On computers, mobile devices or cloud resources
- On networks (data and voice)
- On magnetic or optical storage media (e.g., hard drive, CD, thumb drives)
- In physical storage environments (e.g., offices, filing cabinets, drawers)

If an authorized user is not aware of the security requirements for information to which he or she has access, he or she must provide that information with maximum protection until its requirements can be ascertained.

Any individual who has been given a physical key, ID card or logical identifier (e.g., computer or network account) that enables him or her to access information is responsible for all activities performed by anyone using that key or identifier. Therefore, individuals must be diligent in protecting his or her physical keys and ID cards against theft, and his or her computer and network accounts against unauthorized use. Passwords created for computer and network accounts should be difficult to guess. Furthermore, passwords should never be shared or recorded and stored in a location that is easily accessible by others. Stolen keys and ID cards, and computer and network accounts suspected of being compromised should be immediately reported to the appropriate authorities.

The assignment of a single network or system account to a group of individuals sharing the same password is highly discouraged and may only occur in cases where there is no reasonable, technical alternative.

4. GUIDANCE:

a. **Diligence Concerning Information Associated With "Identity Theft":** Identity theft is a serious and growing problem in our society. Anyone who can obtain certain pieces of information about an individual can obtain credit cards, take out loans, create forged documents or steal assets in the individual's name. Being sensitive to the identity theft threat, the University requires that extra precaution be taken when collecting, using and storing data classified as Level 1 and Level 2 under the *Data Classification Guidelines*, such as but not limited to:

- Social Security Number
- Date of birth
- Place of birth
- Mother's maiden name
- Credit card numbers
- Bank account numbers
- Income tax records
- Driver's license numbers

Collection and use of any of the above pieces of information should be limited to situations where there is legitimate business need**.** Managers must ensure that their faculty and employees understand the need to safeguard this information, and that adequate procedures are in place to minimize this risk. Access to such information may be granted to authorized individuals only on a need-to-know basis.

b. **Limitations on Sharing Personally Identifying Information:** All Level 1 and Level 2 data gathered and maintained by faculty and employees of the University of Portland, for the purpose of conducting University business, that personally identifies any living or deceased individual — names and other personal information pertaining to individual students, faculty, staff, alumni, parents, guardians, spouses, children, donors, beneficiaries, etc. — is considered Level 1 unless otherwise specified by this document or by the appropriate Information Custodian or designate. Such information associated with an individual may be shared only with:

- The individual with respect to whom the information is maintained
- Persons or entities designated by that individual as indicated on a consent form, and consistent with any laws regarding the consent form
- University faculty, employees and representatives (included selected volunteers) who need access to such information for legitimate University business or to support the processing of such information, and who are authorized by the appropriate Information Custodian or designate
- Governmental agencies to which the University has a legal obligation to provide such information
- University-contracted organizations (e.g., health insurers, etc.) that require such information to deliver their services on behalf of the University, are authorized by the appropriate Information Custodian, and

are bound by appropriate, non-disclosure agreements
- Those permitted or required to access the information under applicable laws

c. **Methods of Distributing Level 3 Information Associated with Individuals:** Some pieces of personally identifiable information are considered Level 3 or public information. These pieces of information are described in the ***Data Risk Classification Guidelines***. The following procedures describe how Level 3 information associated with individuals may be shared:

- Directory information, including name, class (students), office address and phone number (faculty and staff) and e-mail address, can be made generally available over the electronic University Web site. The campus address and phone number for any student may also be made available behind an authentication mechanism except for those students who have submitted a formal request to the University to keep such information confidential.

- Directory information of students should not be provided to third parties without first determining whether the student has objected to its disclosure to third parties. If so, his or her directory information must not be disclosed to persons outside the University unless permitted by the Family Educational Rights and Privacy Act. ***NOTE: The Registrar maintains official University records of students who have expressly objected to such disclosure***.

- Other Level 3 information may be released in response to reasonable requests.

d. **Exchanging Information via E-Mail or Other Network Facilities:** Electronic mail (e-mail) is considered an insecure mechanism for exchanging information. The privacy of information contained within e-mail messages can be exposed, especially when either the sender or any of the recipients are off-campus or utilize a wireless network connection. If information, deemed by its Information Custodian as Level 1 or Level 2, must be exchanged with an individual or entity off campus using e-mail or any other network facility that transfers data, it must be encrypted using a hardware or software based mechanism approved by the Vice President for University Operations.

e. **Discarding Information:** Physical documents containing information that has been classified as Level 1 or Level 2 by their Information Custodians and/or designates must be shredded using a University approved device or shredding facility before being discarded. Any computer hard drive or removable magnetic medium, that has been used to hold any kind of Level 1 or Level 2 information must be electronically "scrubbed" using approved software prior to being discarded or being transferred to any individual or entity who is not authorized to view such information. On such media, the mere deletion of Level 1 data is not sufficient because deleted information is still accessible to individuals possessing any number of available software tools. Any nonerasable medium, such as a CD or optical disk that has been used to hold any kind of Level 1 or Level 2 information must be physically destroyed before being discarded. The Vice President for University Operations and the Physical Plant will provide solutions for shredding materials when the volume to be discarded requires their assistance. Information on office shredders is available from the Vice President for University Operations, who has equipment recommendations based on projected volume.

- **Valid Uses of Aggregate Information.** Authorized users may analyze and aggregate institutional data. But official, published reports that include such aggregate data may only be issued with the review and approval of the appropriate Information Custodian. Similarly, sharing those reports with individuals or organizations for which the reports are not primarily intended requires the permission of the individual or office primarily responsible for the report.

- **Subpoenas.** Authorized users are reminded that the full range of information collected on any living or deceased individual—students, faculty, staff, alumni, parents, guardians, spouses, children, donors,

beneficiaries, etc. — in hard copy or electronic form may be subpoenaed and entered into the public record of a court case. Appropriate discretion should therefore be exercised in the drafting of any document that will be stored in any University file including any computer or electronic file. An employee who receives a subpoena, a court order, or any request from a law enforcement agency that requires the disclosure of University held information should contact the Vice President for Student Services or the Vice President for University Operations before taking any action.

- **Reporting of Security Breaches or Suspicious Activity.** Any member of the University staff who comes across any evidence of information being compromised or who detects any suspicious activity that could potentially expose, corrupt or destroy information must report the matter to his or her immediate supervisor and the Vice President for University Operations. No one should take it upon himself or herself to investigate the matter further without the authorization of the Vice President for University Operations.

f. **Additional Requirements for Information Services Personnel:** Information Services staff manage computing and network environments where University information is stored, transmitted or processed, such as:

- Computer operating environments (e.g., UNIX, Windows, Macintosh, etc.)
- Database management environments (e.g., Oracle, Sybase, SQL Server, Access, etc.)
- Application environments (e.g., Banner, Access, etc.)
- Network environments (e.g., electrical, optical, microwave and wireless networks, routers, switches,firewalls, etc.)
- Physical storage facilities (e.g., tape libraries, filing cabinets, etc.)

Information Services is responsible for ensuring that specific data's requirements for confidentiality, integrity and availability as defined by the appropriate Information Custodian are being satisfied within their environments. This includes the development of:

- A cohesive architectural policy
- Product implementation and configuration standards
- Procedures and guidelines for administering network and system accounts and access privileges in a manner that satisfies the security requirements defined by the Information Custodians
- An effective strategy for protecting information against generic threats posed by computer hackers
- An annual audit of user roles and permissions with the assistance of the information custodians so as to ascertain if a level of Banner access is appropriate for the given employee's job responsibilities

5. **EXCEPTIONS:** There are no other exceptions for this policy

6. **SANCTIONS:** Accounts and network access may be administratively suspended by the University with or without notice when, in the University's judgment, continued use of the University's resources may interfere with the work of others, place the University or others at risk, or violate University policy. Any violation of this policy by a student may lead to disciplinary charges under the appropriate student disciplinary policy, which may include expulsion or suspension of student status. Faculty and staff violations will be addressed by their respective disciplinary policies and procedures. All known and/or suspected violations will be reported to the Vice President for University Operations. Users of University of Portland computing facilities are subject not only to University Policies, but also to applicable local, state and federal laws.

Appendix A — Potentially Applicable Legal Constraints

Several federal and state laws may also apply to information collected and maintained by University employees. Laws most likely to apply in our environment are described below.

Computer Fraud and Abuse Act (CFAA)
The CFAA criminalizes unauthorized access to a "protected computer" with the intent to defraud, obtain any information of value or cause damage to the computer. Under the CFAA, a "protected computer" is defined as a computer that is used in interstate or foreign commerce or communication or that is used by or for a financial institution or the government of the United States. For example, the act of "hacking" into a secure web site from an out-of-state computer may violate the CFAA. *The Vice President for University Operations is the university point of contact for CFAA-related issues.*

Electronic Communications Privacy Act (ECPA)
The ECPA broadly prohibits (and makes criminal) the unauthorized use or interception of the contents or substance of wire, oral or electronic communications. In addition, the ECPA prohibits unauthorized access to or disclosure of electronically stored communications or information. Such prohibitions may apply to University employees who willfully exceed the scope of their duties or authorizations by accessing certain databases housed within the University system. The ECPA does not, however, prohibit the University from monitoring network usage levels and patterns in order to ensure the proper functioning of its information systems. *The Vice President for Operations is the University point of contact for ECPA-related issues.*

The Family Educational Rights and Privacy Act (FERPA)
FERPA (also known as the Buckley Amendment) affords students (or parents if the student is a minor) certain rights with respect to the student's "education records." As defined under FERPA, the term "education records" encompasses a broad range of materials and information such as disciplinary, financial, academic, and other records established during a given student's enrollment and maintained in a variety of University databases and other filing arrangements. In particular, FERPA provides that "education records" and personally identifiable information contained therein may not be released or disclosed (including disclosure by word of mouth) without the written consent of the student (or parents, as the case may be). Even in the absence of express student (or parental) consent; however, FERPA permits disclosure of education records to University employees who have a legitimate interest in the student and to outside parties in a variety of circumstances. *The Registrar is the University point of contact for FERPA-related issues.*

Health Insurance Portability and Accountability Act (HIPAA)
Enacted in 1996, HIPAA sets national privacy standards for the protection of certain types of health information to the extent that this information is electronically transmitted by health plans, health care clearinghouses, and health care providers. The University is subject to HIPAA as a provider of employee group health plans. Accordingly, with respect to such health plans, the University has (1) adopted written privacy procedures describing who has access to protected health information, how such information will be used, and when it may be disclosed; (2) required business associates to protect the privacy of such health information; (3) trained employees in the applicable privacy policies and procedures; and (4) designated a privacy officer to be responsible for ensuring that such policies and procedures are followed. HIPAA may also apply to certain research activities such as the collection and use of personally identifying health information from patient populations in clinical settings. *The Vice President of Student Affairs is the designated privacy officer for HIPAA-related issues.*

The Financial Services Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act [GLBA])
The GLBA requires financial institutions to carefully protect customers' financial information. Universities are "financial institutions" by virtue of their loan servicing and therefore must comply with GLBA provisions. The GLBA has two relevant components: (1) "safeguarding" rules and (2) privacy rules. All personally identifiable financial information from students, parents, and employees must be safeguarded against foreseeable risks of disclosure, intrusion and systems failure. The University has designated information security program managers in the business units that handle financial information, identified risks to the security of financial information, and is developing security programs to protect

against risks. GLBA's privacy standards must be followed for all nonstudent financial information. The University has a separate privacy policy to comply with GLBA and makes required privacy notifications to nonstudent customers whose financial information is obtained. *The Controller is the University point of contact for GLBA-related issues.*

The Technology, Education, and Copyright Harmonization Act (TEACH Act)
The TEACH Act relaxes certain copyright restrictions so that accredited, nonprofit colleges and universities may use multimedia content for instructional purposes in technology-mediated settings. But the TEACH Act carries a number of security requirements designed to ensure that digitally transmitted con- tent will be accessible only to students who are properly enrolled in a given course. *The Vice President for University Operations is the University point of contact for TEACH Act-related issues.*

State Laws
In addition to the federal laws summarized above, state laws may apply to the handling of Level 1 information. For example, state laws may govern the collection or use of information regarding children, consumers and other groups. Before establishing new practices regarding the handling of level 1 information, University employees are encouraged to consult the Vice President for Student Services in order to determine whether specific Oregon laws apply.

Subpoenas and Other Compulsory Requests
Many of the federal and state laws described above create exceptions allowing for the disclosure of Level 1 information in order to comply with subpoenas, court orders and other requests from law enforcement agencies. Employees who receive such orders or requests should contact the Vice President for Student Services before taking any action.

Appendix B — Table of Information Custodians and Designated Contacts

As previously stated within this document, the guardian of a logical collection of information is typically the head of the department on whose behalf the information is collected or who is most closely associated with such information. For each assigned information collection, each Information Custodian or individual whom he or she designates is required to:

- Define the collection's requirements for confidentiality, integrity and availability (see Data Risk Classification Guidelines for requirement classifications)
- Convey the collection's requirements in writing to the managers of departments that will have access to the collection
- Work with Deans, Chairs, and Department Heads to determine what users, groups, roles or job functions are authorized to access the information in the collection and in what manner (e.g., who can view the information, who can update the information) and to convey the collection's requirements to any person authorized to access the information
- Authorized users are required to understand the security-related requirements associated with the information with which they come into contact

This following table lists the information collections and their custodian:

Information Collections Pertaining to…	**Information Custodian**
Students:	
The physical or mental health of any University student	Director of Health Center
Applicants — Undergraduates	Dean of Admissions
Applicants — Graduates	Dean of Graduate School
Athletes	Athletic Director

Graduate Students	Registrar
Undergraduate Students	Registrar
Financial Aid	Director of Financial Aid
Faculty and Staff:	
Work-related injuries for active employees or those on long-term and short-term disability	Vice President for Human Resources
Applicants — Faculty and related staff	Academic Deans
Applicants — Staff	Vice President for Human Resources
Current Faculty and related staff	Academic Deans
Current Staff	Vice President for Human Resources
Dependents and beneficiaries of Faculty and Staff	Vice President for Human Resources
Alumni, Donors, Parents:	
Alumni (Personal Information)	Director of Alumni Relations
Donors (including potential donors), Parents, Constituents	Vice President for University Relations
University Operations:	
Academic/Administrative Departments Community Affairs Facilities Financial Matters Information Technology Legal Matters Library Records, Archives, and Museum Campus Safety	Head of the appropriate department Vice President of Marketing Director of Physical Plant Vice President for Financial Affairs Vice President for University Operations Vice President and Legal Counsel Dean of Library Director of Campus Safety