Oregon State Board of Higher Education
Policy Guidelines for Electronic Commerce

Policy Guidelines for Electronic Commerce

The Oregon State Board of Higher Education (Board) views electronic commerce as a natural extension of the business processes already conducted by the Board and its seven universities (System). The Board encourages System universities to utilize electronic commerce to improve service to its students, faculty, staff and the public, and to reduce the cost of providing these services. For purposes of this policy, electronic commerce includes all business_transactions accomplished using an electronic medium. In all endeavors of this type,'the System shall protect the assets of the State, the integrity of the data, the financial and confidential information about the customer, and preserve the trust and confidence in using electronic commerce. This requires an appropriate combination of System and institutional management oversight, and includes sound policies, procedures, technologies, and internal controls.

Authority

ORS 291.038, OAR 580-040-0005

Application of the Policv

This policy applies Systemwide to all financial transactions performed using an electronic medium which involve use of System facilities, personnel, or other resources.

Assignment of Responsibility

(1) The Vice Chancellor for Finance and Administration or designee shall have oversight responsibility for System provisions as set forth in this policy, and for provisions relative to Chancellor's Office electronic commerce activities.

Each university Vice President for Finance and Administration or designee shall have oversight responsibility on their campus for institutional provisions set forth in this policy.

Standards

The Board affirms the need for consistency across all institutions in certain electronic commerce business activities and also recognizes the need for flexibility in others. In furtherance of these objectives, the Board establishes the following standards:

(1) Each Campus shall develop a privacy statement in accordance with the Federal Family Educational Rights and Privacy Act of 1974 (FFERPA) and complimentary to the DAS privacy statement.

(2) Accounting practices for electronic commerce transactions shall adhere to appropriate accounting standards as established by the Vice Chancellor for Finance and Administration.

(3) Financial information transmitted electronically shall be sent using an appropriate level of security. The security technologies used shall, at a minimum, be consistent with standards established by the Oregon State Treasury and meet or exceed common industry standards.

(4) Credit card authentication shall be performed through a verification service approved by the Oregon State Treasury.

(5) Sensitive data, including social security numbers, credit card numbers, passwords, and any other similar data whose compromise would have a material negative impact, shall be stored in a secure format unless otherwise approved by the institution's Vice President for Finance and Administration or designee.

(6) All transactions shall be uniquely serialized and fully journaled to provide a conclusive audit trail.

(7) All goods and services provided and received shall be routinely reconciled with the accounting records.

(8) All applications shall comply with all current Board and pertinent State of Oregon public procurement statutes, rules, and regulations. Outsourced core applications shall meet the standards specified by the Vice Chancellor for Finance and Administration or designee. Outsourced peripheral applications shall meet the standards specified by the institution's Vice President for Finance and Administration or designee.

(9) In house applications shall occur on limited access systems rather than on general purpose systems (which may be used for miscellaneous other purposes such as e-mail, web hosting, etc.).

(10) Any non-System advertising connected with electronic commerce shall be approved in accordance with institutional policies.

(I1) Electronic commerce systems shall be fully and securely archived

(12) Any effort to divert electronic commerce revenues or compromise systems associated with electronic commerce activities shall be subject to prosecution under Oregon Revised Statues pertaining to theft, alteration of public records, or other applicable laws.

(13) The System shall periodically review this policy for consistency with DAS policies.

Oregon State Board of Higher Education
Policy Guidelines for Electronic Commerce

Definitions

(1) Core Application: An activity which is closely integrated with already deployed student information systems, financial information systems, and/or human resources information systems. It is central to the institution's mission and revenue stream, and is directly and substantially related to students. A core application is usually:

- high dollar volume (hundreds/thousands of dollars);
- high transaction frequency (thousands of transactions);
- broad scope (activity is institution-wide);
- high degree of integration with existing systems (uses existmg dedicated computing systems).

Examples of core applications would include tuition payments, housing payments, and fee payments.

(2) Electronic Commerce: A broad term used to describe business transactions conducted using an electronic medium.

(3) Electronic Medium: Mechanism for transferring, stonng, and manipulating electronic data using facilities and devices such as telephone, lease lines, the Internet, compact disc, magnetic tape, diskettes, and fiber lines.

(4) In-house Application: System owned or licensed software running on System controlled hardware.

(5) Limited Access Svstem: A server with a dedicated purpose allowing access only to individuals with system critical needs.

(6) Peripheral Application: An activity which is not closely integrated with already deployed student information systems, financial information systems, and/or human resources information systems. It is occasional and incidental to the institution's mission and revenue stream. A peripheral application is usually:

- low dollar volume (tens of dollars);
- low transaction frequency (tens of transactions);
- limited scope (activity is unique to a particular department);
- low degree of integration with existing systems (no existing dedicated computing systems).

An example of a peripheral application would be the sale of a technical report by an academic department.

(1) Security/Secure: Authorization and verification of users, assuring integrity of transaction, and encryption (the conversion of data into a proprietary code or accepted open source standard for security purposes.)