

IT01 University of Oregon Policy Guideline for Electronic Commerce

Effective 22 Mar 2001

Last Revised 4 June 2002

Who Should Read This Policy

Anyone processing University of Oregon financial transactions using an electronic medium, which involves the use of University facilities, personnel, or other resources.

Background & Purpose

The Business Affairs Office views electronic commerce as a natural extension of the business processes already conducted by the University. The Business Affairs Office encourages Colleges and auxiliary departments to utilize electronic commerce to improve service to 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 the University shall protect and preserve:

- the assets of the state,
- the integrity of the data,
- financial and confidential information about the customer, and
- customer trust and confidence in using electronic commerce.

This requires an appropriate combination of Oregon University System and institutional management oversight, including sound policies, procedures, technologies, and internal controls.

Policy

To achieve consistency across OUS institutions in certain electronic commerce business activities and recognize the need for flexibility in others, the University of Oregon will abide by the following standards:

1. 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. Adhere to appropriate accounting standards as established by the Vice Chancellor for Finance for electronic commerce transactions.
3. Transmit financial information electronically 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. Use a verification service approved by the Oregon State Treasury to authenticate credit card, debit card and electronic check transactions.
5. Securely store sensitive data, (including social security numbers, credit card numbers, passwords, and any other similar data) whose compromise would have a material negative impact, in a secure format unless otherwise approved by the Vice President for Finance and Administration or designee.
6. Uniquely serialized and fully journalize all transactions to provide a conclusive audit trail.
7. Routinely reconcile all goods and services provided and received with the accounting records.
8. Comply with OUS Board and State of Oregon procurement statutes, rules, and regulations in all applications.
9. When outsourcing:
 - Meet the standards specified by the Vice Chancellor for Finance and Administration when outsourcing core applications, and
 - Meet the standards specified by the institution's Vice President for Finance and Administration or designee when outsourcing peripheral applications.
10. Host in house applications on dedicated, limited access systems rather than on general purpose systems (which may be used for miscellaneous other purposes (such as e-mail web hosting, etc.).
11. Restrict non-University advertising to that which is approved in accordance with University policies.
12. Fully and securely archive electronic commerce systems.
13. Subject any attempt to divert electronic commerce revenues or compromise systems to prosecution under Oregon Revised Statutes pertaining to theft, alteration of public records, or other applicable laws.
14. Periodically review this policy for consistency with OUS and DAS policies.

Authority

The UO Vice President for Finance and Administration has authority for administering this policy and has delegated its implementation to the Director of Business Affairs.

References

FASOM Section 14.01 Policy guidelines for electronic commerce.
UO eCommerce Privacy Statement,
<http://baowww.uoregon.edu/Policy/ecommpolicy.htm>
OAR 580-040-0005 State Board delegation and assignment of financial responsibility.
ORS 291.038 State agency planning, acquisition, installation and use of information and telecommunications technology; integrated video conferencing; on-line access service; Stakeholders Advisory Committee; rules.

Related State Policy:

- Governor's Executive Order 00-30 Electronic Government
- DAS Policy 03-27 Electronic Commerce: Applications involving Electronic Transmission of Credit Card Data Over the Public Internet
- Oregon House Bill 2039 Uniform Electronic Transactions Act

Related Procedures

The following practices should be considered:

- Increase public access to government information by making frequently requested government information available online;
- Acquire technology that is adaptable and interoperable;
- Foster partnerships;
- Select open architecture solutions that are designed for long term growth and utility;
- Make information accessible through shared network infrastructure;
- Design system flexibility that allows users to develop unique solutions that suit individual needs;
- Reduce transaction times for those using government services;
- Leverage State information technology investments to benefit multiple agencies, governments and its citizens;
- Get the maximum benefit of current information and technology;
- Improve opportunities for enterprise growth and development; and
- Increase the quality and quantity of distance learning offerings.
- Reduce operating costs.

Q&A

What services does the Business Affairs Office offer to UO departments and what do these services cost?

The Business Affairs Office offers a range of services:

- technical consulting,
- payment processing,
- application development, and
- application hosting.

Fees are negotiated on a cost recovery basis for all services delivered.

Compliance Examples

Example 1 Department A decides to sell a product via the web. Department A has sufficient technical resources to host an ecommerce application so they purchase a dedicated ecommerce server, server software, and contract with a credit payment verification service that is approved by the Oregon State Treasury. In doing so they comply with OUS Board and State of Oregon procurement statutes, rules, and regulations. They build and host their own electronic storefront. They securely store and archive all data. They restrict non-University advertising to that which is approved in accordance with University or Oregon policies. They transmit financial information electronically using an appropriate level of security (secure sockets layer), publish an appropriate privacy statement and adhere to appropriate accounting standards as established by the Vice Chancellor for Finance and Administration for electronic commerce transactions.

Example 2 Department B decides to sell a product via the web. Department B has insufficient technical resources to host an ecommerce application so they contract with a third party and outsource for ecommerce services. If the product is closely integrated with already deployed student, financial, or human resources information systems, or is central to the institution's mission and revenue stream, and is directly and substantially related to students they consult with and meet the standards specified by the Vice Chancellor for Finance and Administration. If the product is not closely integrated with already deployed student, financial, or human resources information systems, and is occasional and incidental to the institution's mission and revenue stream, and is not directly and substantially related to students they consult with and meet the standards specified by the University of Oregon Vice President for Finance and Administration.

Example 3 Department C decides to sell a product or accept payment for a service via the web. Department C has insufficient technical resources to host an ecommerce application so they contract with the Business Affairs Office for ecommerce support. The Business Affairs Office provides credit verification and payment services and, if appropriate, publishes Department C's products on the University of Oregon ecommerce server storefront. Department C delivers the product to fill the order.

Contact

eCommerce Coordinator, 346-6249

Definitions

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 existing dedicated computing systems).

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

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

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

In-house Application System owned or licensed software running on System controlled hardware.

Limited Access System A server with a dedicated purpose allowing access only to individuals with system critical needs.

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.

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.)