1. Call to Order/Roll Call/Welcome .................................................................................................. 1
2. Action Items .................................................................................................................................. 1
   a. OSU, Lease and Renovation Project, Hewlett-Packard Building 11................................. 1
   b. PSU, Academic and Student Recreation Center (PCAT development)......................... 4
3. Discussion Item .......................................................................................................................... 7
   a. OAR 580-XXX-0000, OUS Information Security – Proposed Policies ......................... 7
4. Adjournment .............................................................................................................................. 17
MINUTES OF THE BOARD FINANCE & ADMINISTRATION
COMMITTEE MEETING
WESTERN OREGON UNIVERSITY, MONMOUTH, OR
APRIL 6, 2007

MINUTES

1. CALL TO ORDER/ROLL CALL/WELCOME

Chair Don Blair called the meeting of the Board Finance and Administration Committee to order at 9:06 a.m.

Committee Members present included Chair Don Blair and Directors Henry Lorenzen and John von Schlegell. Director Tony Van Vliet was also present.

Chancellor’s Office staff present included: Chancellor George Pernsteiner, Jay Kenton, Bob Simonton, and Ryan Hagemann. Others present included: presidents Dan Bernstine (PSU), Mary Cullinan (SOU), Khosrow Fatemi (EOU), John Minahan (WOU), and Ed Ray (OSU). Provost Dave Woodall (OIT) and Vice Presidents Lindsay Desrochers (PSU), Frances Dyke (UO), and Mark McCambridge (OSU) were also present.

2. ACTION ITEMS

a. OSU, Lease and Renovation Project, Hewlett-Packard Building 11

DOCKET ITEM:

Summary:
Oregon State University sought Board approval to redirect bonding authority to renovate approximately 30,000 square feet of laboratory space for ONAMI-related research from Graf Hall to Building 11 (B-11) on the Hewlett-Packard (HP) Corvallis campus. OSU currently occupies approximately one-quarter of the building under a license agreement with HP. In addition to operating ONAMI-related laboratories in B-11, OSU hosts the ONAMI Inc. Executive Offices, provides space for ONAMI collaborators from other Oregon university partners, and sublicenses space to Pacific Northwest National Laboratories as part of PNNL’s collaboration with OSU/ONAMI. OSU’s ONAMI-related goals for research and commercialization require the additional space offered by full use of B-11. Accordingly, OSU proposes to enter into a long-term lease agreement with HP and renovate B-11. Under terms of the lease, OSU will receive free rent and pay only operating expenses.
Background:
Initial project scoping with researchers indicated that 30,000 to 32,000 sq. ft. of laboratory space would be needed. Based on preliminary evaluations, it was felt that approximately 30,000 sq. ft. of flexible laboratory space and offices could be constructed within the roughly 40,000 sq. ft. Graf Hall shell at a cost of about $300 per sq. ft. (net). In 2003, the Oregon legislature approved $4.75 million in Article XI-G bonds, $4.75 million in Lottery bonds, and $9.5 million in Other Funds to renovate Graf Hall in support of a nanotechnology and micro-products research and development center, since renamed the Oregon Nanoscience and Microtechnologies Institute (ONAMI)–OSU.

More detailed engineering analysis of Graf Hall showed that significant seismic upgrades were required and that these upgrades, together with the mechanical equipment and ADA requirements of the proposed laboratories, would reduce the available space to about 25,000 sq. ft. The envisioned research and development activities could not be accommodated in that space.

Various Graf Hall renovation design alternatives were investigated and at least one alternative allowed nearly 30,000 sq. ft. of available space; however the estimated cost of this alternative was between $17.5 and $22.5 million. This scenario would require raising $8 to $13 million and significantly delay the project.

A new construction alternative was also investigated. Preliminary estimates suggested that a new 50,000 sq. ft (gross) building could be constructed for approximately $25 – 30 million to meet the needs of the researchers. Beyond requiring the approval of the Board and the legislature, this scenario would require raising roughly $15-20 million and delay the research.

While these alternatives were investigated, an agreement was reached with HP in June 2004 to allow OSU the use of 21,500 gross sq. ft. of space in B-11 on the Corvallis HP campus. HP provided the space without cost to OSU in support of the ONAMI-related research. Approximately 8,750 sq. ft. of laboratory space was developed at a cost of about $1.2 million and existing office space totaling 12,700 sq. ft. is occupied by OSU researchers.

In August 2005, PNNL entered into an agreement with OSU to sub-license a portion of the B-11 laboratory and office space to collaborate with OSU researchers. PNNL constructed approximately 1,800 sq. ft. of access-controlled laboratory space within the space OSU developed in 2004.

In 2006, HP indicated a willingness to enter into a long-term lease for all of B-11 with OSU. The terms of the lease would allow OSU to meet the goals of the original Graf Hall renovation project within the limits of the bonding authority authorized in 2003.

Terms of the Proposed Transaction and Legal Considerations:
The B-11 facility is located at 1000 NE Circle Blvd, Corvallis, Oregon, and consists of 83,511 gross sq. ft.; 70,797 sq. ft. on the ground floor and 12,714 sq. ft. of office space on the second floor. Terms of the proposed 20-year lease agreement would allow HP to recover only expenses
associated with maintenance and operation of B-11 and the common areas to which OSU would have access under the lease. HP has estimated those costs currently to be $300,000 annually. Commercially available space in the Corvallis area leases for $18 to $20 per sq. ft. per year. (HP plans to lease a portion of an adjacent building for $18.50/ft/year.) Using a $19 rate, B-11 would lease for in excess of $1.5 million per year. Assuming the estimated annual operating expenses are correct, OSU will save in excess of $1 million per year.

Once the building is leased, OSU proposes to use the $9.5 million (from lottery and Article XI-G bonds) to renovate approximately 30,000 sq. ft. of space for laboratories and supporting infrastructure. This newly renovated space, combined with the existing 8,700 sq. ft., will bring the total laboratory space to approximately 39,000, which should be sufficient for current research needs. A feasibility study conducted as part of this project identified another 13,000 sq. ft. within this facility that could be developed in the future.

**Staff Recommendations to the Finance and Administration Committee**

Staff recommended that the Board Finance and Administration Committee approve the project actions as outlined below and subsequently recommend to the full Board for approval.

1. Approve OSU’s proposed 20-year lease with Hewlett Packard for the use of this facility to house the Oregon Nanoscience and Microtechnologies Institute.
2. Authorize the Chancellor, or designee, to seek authority from the legislature to transfer $4.75 million of Article XI-G bonds, $4.75 million of Lottery bonds, and $9.5 million of Other Funds spending limitation from the Graf Hall Renovation Project, approved in the 2003-2005 biennium, to the B-11 Renovation Project, located on the Hewlett Packard-Corvallis Campus.

**COMMITTEE DISCUSSION AND ACTION:**

Robert Simonton, Associate Vice Chancellor, summarized OSU's request to modify the Graf Hall project. He indicated that, after consultation with the Department of Justice and DAS, this request is legally permissible. The following steps are required before the project can move forward: 1) Board approval of a 30-year lease and 2) permission to seek authority from the legislature to modify the current capital budget request and redirect bond proceeds to the new modified project.

Vice President Mark McCambridge from OSU explained that HP is "basically providing $18-19 a foot free of charge to OSU, calculated at about a million dollars a year. Over a 30-year period, OSU is gaining 83,000 square feet of usable space at a $30 million savings. So, we think it is an excellent idea."

Attempting to clarify the financial numbers, Chair Blair asked if the original project was a $19 million project and that OSU basically has about $10.5 million in cash. “What happens with Graf Hall and what goes on there?” he inquired. Dr. Ron Adams, Dean of the School of Engineering, indicated that Graf Hall is an engineering building that contains laboratories.
predominantly for civil and mechanical engineering and if the Board approves the current request, it will continue to be used for those purposes.

Director von Schlegell asked if there were any other connections between HP and OSU. Dean Adams responded that HP is “our best corporate partner and we have a number of collaborative research projects with them. They are also collaborating in some of the other ONAMI projects. There is a partnership that goes beyond the current lease agreement request.”

To affirm that this project was still a priority, Chair Blair reminded members that “we’re being challenged to make sure that whenever we’re spending the state’s capital that we are spending it on the things that we think are most important. ONAMI is one of the things that we’ve identified as an area of investment for the System and a place where we can develop some competitive advantage. I do believe this is on strategy but we’re also continuously reaffirming that this is one of the things that we think it is important to fund,” he concluded.

Director von Schlegell moved and Director Lorenzen seconded the motion to approve the staff recommendation and forward the item for full Board approval. Those voting in favor: Directors Blair, Lorenzen, and von Schlegell. Those voting no or abstaining, none. Motion passed.

b. ................................................................................................................................................. P
   SU, Academic and Student Recreation Center (PCAT development)

DOCKET ITEM:

Summary
In July 2006, Portland State University (PSU) received approval from the Board for a capital construction project that would redevelop the block currently occupied by the University’s Portland Center for Advanced Technology (PCAT), located on Southwest Fifth and Sixth Avenues in Portland. The project, currently titled the Academic and Student Recreation Center, is a mixed-use project situated on the plaza adjacent to PSU’s Urban Center. In November 2006, the OUS Board approved a revision that divided the project into two phases. The first phase totals $51 million and commences in Spring 2007. The project is currently in early design. The second phase would commence upon availability of funding and total up to $30 million contingent upon the final approvals of the Governor and legislature. PSU sought Board approval to increase the Other Funds limitation for Phase I of the project by $13.5 million to accommodate inclusion of space for the City of Portland’s historical records archive.

Background
The Archives and Records Management section of the City of Portland Auditor’s Office is responsible for maintaining all official business records for the City. This function is currently housed in the Stanley Parr Archives and Records Center (SPARC) located at Chimney Park, 9360 North Columbia Boulevard in Portland, Oregon. SPARC professional staff provide specialized reference assistance and research for City bureaus, private citizens, and other entities, providing guidance and help in searches for both current and past public information.
The City’s current facility is 10,000 square feet and was originally constructed in 1932. The City’s need for archives and records storage has exceeded the current capacity of the SPARC Building and a recent feasibility report prepared for the City by Oh Planning + Design indicates a need for approximately 28,000 square feet, including research, office, and support space. The current location of Archives and Records Management in North Portland is not convenient for most users. Relocating this function to the Academic and Student Recreation Center site would make it more central, as well as provide close proximity to City Hall and other municipal functions. The Academic and Student Recreation Center site’s location at a central transit hub would allow convenient access via the Central City Streetcar, as well as the new TriMet MAX Green Line that is currently under construction.

The City and PSU anticipate that significant joint benefits could be achieved by relocating the historical records to the University. Having the historical records on campus would be a major stimulus to on-campus research among undergraduates, graduates, and faculty. The historical records location would also be in close proximity to the University’s College of Urban and Public Affairs, the Center for Urban Studies, the Center for Columbia River History, and the Institute of Portland Metropolitan Studies, allowing for a wide range of potential collaborative relationships, seminars, and joint research proposals. Faculty and students from a wide variety of disciplines, including history, political science, environmental science, criminology and criminal justice, sociology, anthropology, conflict resolution, social work, and civil engineering would benefit from the presence of the Archives close proximity. The historical records would also provide a significant source of support for PSU’s visiting scholars, as well as encourage visitations from independent legal and scholarly entities interested in accessing the facility for research.

Terms of the Proposed Transaction and Legal Considerations:
The City of Portland and PSU are proposing a revision to the Academic and Student Recreation Center project to include approximately 28,000 square feet of storage, office, and public research space for the Archives. The City is prepared to finance the full costs of required additional design and construction. The resulting structure would, pending final discussions with the City, be configured as a six-story condominium, similar to the current condominium arrangement between the City and PSU in the Fourth Avenue Building.

The revised funding plan is as follows:

<p>| | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Student Recreation Center</strong></td>
<td><strong>Article XI-F(1) Bonds</strong></td>
<td><strong>Student Recreation and Building Fees</strong></td>
<td>$35,000,000</td>
</tr>
<tr>
<td><strong>Retail Space</strong></td>
<td><strong>Article XI-F(1) Bonds</strong></td>
<td><strong>Lease Revenues</strong></td>
<td>7,000,000</td>
</tr>
<tr>
<td><strong>Classroom/Chancellor’s Office Space</strong></td>
<td><strong>Chancellor’s Office Fund Balance</strong></td>
<td></td>
<td>3,000,000</td>
</tr>
</tbody>
</table>
Chancellor’s Short-term Loan ........................................... 3,000,000
Additional Funds:
City of Portland ........................................................... 2,000,000

Other Sources
Legal Settlement,
Energy Tax Credits, ad Other ........................................... 1,000,000
Original Project Phase I ............................................... $51,000,000
(approved 11/3/06)

City of Portland Archives
City of Portland ........................................................... 13,500,000

Revised Project Phase I ............................................... $64,500,000

PSU has consulted with the Department of Justice and OUS Bond council, who have opined that the City’s funding of the additional design and construction could be used to match Article XI-G bonds since there is a direct and strong link between the University’s mission and the historical records. A memorandum of understanding will be developed to formalize the relationship between the University and the City. To be eligible for Article XI-G funding, Counsel noted that the building would need to be designated as a higher education facility in the authorizing legislation with a condo interest.

The following conditions remain open and must be satisfactorily resolved:
- Negotiations and legal sufficiency review of a memorandum of understanding;
- Approval by the State Board of Higher Education;
- Formal design and costing of Archival space; and
- Approval by the Portland City Council.

Staff Recommendation to the Budget and Finance Committee
Staff recommended that the Finance and Administration Committee approve this concept and subsequently recommend that the full Board take the following actions via its consent agenda:

1. Authorize Portland State University to seek City Council approval of the funding for their new archives to be located in this facility and, assuming such approval is granted, to negotiate a condominium agreement that is satisfactory to all parties.
2. Approve the revised project scope for Phase I of the Academic and Student Recreation Center to include approximately 28,000 square feet of archive space for the City of Portland with an added Other Funds expenditure limitation of $13.5 million.
3. Authorize the Chancellor, or designee, to seek an additional $13.5 million of Other Funds expenditure limitation from the legislature, bringing the revised project limitation to $64.5 million for Phase I of the project.
COMMITTEE DISCUSSION AND ACTION:

PSU Vice President Desrochers reviewed the docket item for the Committee and President Bernstine affirmed that this was a unique opportunity for PSU and that the timing of the PSU project and the need of the City of Portland were mutually advantageous.

Ms. Desrochers indicated that the approximate costs are between $10.5-$11 million, but that PSU has asked for the limitation up to $13 million to assure that the project is funded in the right range. “The proposal is for a condominium arrangement. So for the space the City would occupy, the 24,000-28,000 square feet, they would own. There would be an agreement attached to the condominium agreement for joint use in the common areas, the corridors, elevators, and so forth,” she clarified. If the City should decide to sell their interest in the building, PSU would have a right of first refusal to purchase the property back at an established, agree-upon methodology for the purchase.

To Director Van Vliet's question of the legality of matching another public entity with PSU as a public entity, Ms. Desrochers responded that the Bond Counsel believes it is legal. "There are already City funds in this project. The Portland Development Commission has $2 million invested as part of the overall package for the first part of this project. With regard to the Article XI-G bonds, we wanted to know whether or not those City bonds could be used to match, if it was possible to obtain Article XI-G-bonds, and the Bond Counsel said that they were.”

Chair Blair indicated that the project seemed reasonable to him. He wanted assurance that as PSU goes through negotiations they make sure they have anticipated all of the implications of this agreement over the long term, in fact, in perpetuity. “This cannot end up somehow creating a drain on Portland State resources at some point. But with the assumption that you can negotiate that sort of agreement, I think that there are a lot of benefits for the University and for the City,” he concluded.

It was moved by Director von Schlegell and seconded by Chair Blair to approve the staff recommendation and forward the item to the full Board for approval. Those voting in favor: Directors Blair, Lorenzen, and von Schlegell. Those voting no or abstaining: none. Motion passed.

3. DISCUSSION ITEM

a. OAR 580-XXX-0000, OUS Information Security – Proposed Policies

DOCKET ITEM:

Background
In August 2006, the OUS Internal Audit Division completed a review of OUS information security. This review found that the OUS policy framework did not have comprehensive policies
governing information security and recommended that we develop such policies governing campus operations.

Following this review, the Vice Chancellor for Finance and Administration consulted with the chief information officers at the various OUS institutions and received recommendations of staff with expertise and an interest in this area who could serve on a task force to develop polices of this nature. This group, led by Jon Dolan, Associate Director of Network Services at OSU, included Craig Schiller, Chief Information Security Officer at PSU; John Kemp, Senior Security Engineer at UO; and Andy Abbott, Chief Information Officer at OIT. Although this subcommittee was staffed by information technology professionals, it has a broader application to all forms of information media, including paper copies. This group drafted the following policy framework during the fall term 2006. During this process they reviewed numerous information security policies in place at other universities and other organizations throughout the nation and discussed various options with colleagues throughout OUS. The initial policy framework was circulated among OUS IT professionals, records managers, and others for review and comment.

Once the policy draft was finalized by this group, it was presented to the OUS CIOs for final discussion and acceptance. After this was completed the administrative, provosts, and presidents councils reviewed it. All groups indicated that it seemed comprehensive in scope and although concerns were voiced regarding available resources, disaster recovery/business continuity, and the role of the chief information security officer, all agreed that the policy framework seemed workable, assuming that compliance expectations would be reasonable given these constraints and concerns.

It is proposed that OUS adopt an umbrella information security policy under which each university will adopt specific policies governing campus operations in compliance with this overarching policy framework. This is the first reading of this proposed Oregon Administrative Rule with the Board. It is being presented for discussion purposes at the April meeting and, assuming that it receives a favorable hearing, it will be proposed for adoption as an OUS Administrative Rule at the June 2007 OUS Board meeting.

DIVISION XX
OUS INFORMATION SECURITY POLICIES

Executive Summary

580-XXX-0000

(1) OUS has a responsibility to protect its Information Assets, business processes, and follow appropriate laws and regulation relating to information security.

(2) OUS will meet its obligations by each member institution implementing an ongoing information security program.

(3) Each institution’s President (or designee) will have overall responsibility for its institution’s program.

(4) Each institution will assign Chief Information Security Officer (CISO) duties to a qualified person.
(5) Each institution’s CISO, or equivalent, will be responsible for the security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, and maintained.

(6) Each institution will create Information Systems Policies that cover at a minimum: Classification Standards that at least identify Essential and Highly Sensitive data, processes, and systems; security baselines commensurate with classification; and labeling and handling standards for Highly Sensitive data, processes, and systems.

(7) Each institution will create Personal Information and User Policies that cover at a minimum: Securing Personally Identifiable Information; Acceptable Use of Computing Resources; employee polices for security-sensitive personnel; and account management policies.

(8) Each institution will create Security Operations policies that cover at a minimum: a notification and escalation plan for breaches of personally identifiable information; a risk assessment program; and an incident response plan.

(9) Each institution will create Network and Telecommunications Policies that, at a minimum, ensure that Highly Sensitive Information Assets are in a secured zone on the network and are not transmitted outside of secured zones in clear text.

(10) Each institution will establish physical security standards that protect Essential or Highly Sensitive Information Assets that are critical to the functioning of the institution and ensure that disposal procedures remove or render sensitive data irretrievable from hard drives, compact disks, external memory, PDAs, etc.

(11) Each institution will establish a Disaster Recovery Plan for Essential Information Assets.

(12) Each institution will develop awareness and training programs for all Information Asset users regarding Information Security.

(13) OUS Internal Audit will conduct periodic Information Security Policy Audits.

**Purpose**

580-XXX-0010

The Oregon University System and its member institutions, collectively referred hereinafter as OUS, have a responsibly to protect information entrusted to them, ensure the effective operation of business critical processes, and must abide by the security policies established by the State Board of Higher Education, as well as laws and regulations at the federal, state, and local levels relating to information security. OUS must meet a standard of due care regarding the protection of institutional information assets as well as those belonging to OUS students, faculty members, customers, and research partners.

OUS “Information Assets” include information and systems that are owned by OUS, information that OUS is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. OUS Information Assets are found in written, spoken, electronic, printed, magnetic, optical, and other mediums.

The purpose of this policy is to document OUS management’s intent regarding the protection of these Information Assets. It is to be used by each OUS institutions’ management to develop, document, implement, and maintain local information security policy and programs.
Goals
580-XXX-0020
OUS member institutions will develop and implement ongoing information security programs, and assign clear and appropriate roles and responsibilities to the administration, IT personnel, and institutional community members. The basic objectives are to achieve and maintain:
(1) TRUST—Ensure that institutions establish a baseline of security that will serve as a basis for the ongoing trust of OUS’ information systems, engender confidence between OUS and its students, faculty members, customers, research partners, and the citizens of the State of Oregon.
(2) INTEGRITY—Establish the concepts of due care, best practice, and security baselines as the basis for protecting the Information Assets of OUS in a manner commensurate with their sensitivity, value, and criticality to ensure they meet expectations of form, fit, and function.
(3) ACCOUNTABILITY—Maintain the accountability of information users, preserve management options if there is asset misuse or abuse, ensure security of OUS’s physical assets, and provide for business continuity.

Authority and Scope
580-XXX-0030
This policy applies to the Oregon University System as organized and empowered by ORS Chapters 351 and 352 and is specifically authorized under ORS 351.087. This policy is applicable to all OUS member institutions as well as all employees, students, contractors, consultants, agents, and vendors working on their behalf. It is applicable to all OUS Information Assets, regardless of form or media. It applies to information gathering, protection, use, processing, storage, communications, and transit.

OUS member institution policies, procedures, standards, and work instructions are required to comply with this policy.

580-XXX-0040
Roles and Responsibilities
(1) The OUS Chancellor shall have overall oversight responsibility for the provisions of this policy.
(2) The OUS Chief Information Security Officer (CISO) shall have responsibility to develop, implement, maintain, and monitor compliance with this policy.
(3) Each member institution’s President shall have overall oversight responsibility for institutional provisions set forth in this policy.
(4) Each member institution’s Chief Information Officer (CIO), or equivalent, shall be responsible for ensuring that institutional policies are developed in accordance with this policy.
(5) Each member institution shall designate a CISO or equivalent. The institutions’ CISO shall be responsible for the member institution’s security program and for ensuring that institutional policies, procedures, and standards are developed, implemented, and maintained.
(6) All university community members have a responsibility to help ensure security of the Institution’s Information Assets.

Institutional Policy Requirements
580-XXX-0040

(1) Security Management
(a) Each member institution shall establish an ongoing information security program and assign clear and appropriate roles and responsibilities to their Administration, CIOs (or equivalent), CISO (or equivalent), and all local University community members. The President of each member institution (or their designee) will be responsible for establishing the program and ensuring that it is effective.
(b) Each member institution should create clear and consistent policy in accordance with their information security program, that outline general information security operations including such things as risk assessment procedures, incident response responsibilities, security testing, and day-to-day security compliance. The specifics of those policy requirements are outlined in the following sections.

(2) Information Systems Security
(a) Information Systems are composed of three major components: data, applications, and infrastructure systems. All three must be addressed in order to ensure overall security of these assets. OUS member institutions should establish policy, procedures, security controls, and standards that govern these assets. These policies should ensure that fundamental security principles, such as those documented as pervasive principles in the Generally Accepted Information Security Principles or those generally incorporated into the COBIT framework, are established and maintained.
(b) At a minimum each member institution shall establish:
(A) Information system classification standards. These standards shall ensure that Essential and/or Highly Sensitive data, applications, and infrastructure systems are identified and standards for handling them are developed. Member institutions may deem it appropriate to establish multiple levels of sensitivity or criticality.
(B) Security baselines for information systems. Security baselines are a minimum set of operational guidelines that affect the relative security of an Information Asset. Baselines shall be appropriate to the level of sensitivity and criticality of the systems and ensure that the due care and best practice principles are met.

(3) User and Personal Information Security
(a) Everyone interacting with information assets has a responsibility to ensure the security of those assets. Each member institution must create policies that articulate the rights, responsibilities, and roles of anyone interacting with Information Assets. Policies must take into account federal, state, and local laws, as well as other institutional policies. For example, FERPA requirements will require attention when dealing with student records and HIPPA requirements will require attention when dealing with health information. Policies should be made readily available to all interested parties.
(b) At a minimum each member institution shall establish:
(A) Personal Information Policies. Member institutions are required to specifically define procedures for dealing with personally identifiable information. Information, such as social security numbers, credit card numbers, and driver’s license information, is naturally sensitive and appropriate steps should be taken to protect the privacy of this type of information.
(B) Acceptable Use Policies. Member institutions are required to develop policies that define the parameters of acceptable use for all users of information resources within the organization. These policies must ensure that the use of Information Assets is consistent with standard
security practices, ensures that those resources operate effectively, and that appropriate laws relating to Information Assets are followed. For example these policies may include user resource use limitation, definitions of inappropriate behavior, copyright restrictions, commercial use restrictions, and confidentiality requirements. These polices should also include definitions of enforcement mechanisms in case of violation. Member institutions shall make it clear that prior notification is not a requirement for applicability of the policy and they shall clearly state that there should be no expectation of privacy while using institutional resources.
(C) Security Sensitive Personnel Policies. Employees who have access to essential or highly sensitive data and processes should be designated as serving in critical or security-sensitive capacities as per OAR 580-023-0005 through 580-023-0065 and be subject to the appropriate employment policies of the institution.
(D) Account Management Polices. Member institutions are required to develop policies that ensure appropriate management of user accounts. These polices shall: establish and maintain accountability, timely notification of access changes and terminations, timely response to these notifications, and periodic reconciliation of accounts to active users, privileges, and separation of duty requirements. This includes students, employees, contractors, and vendors.
(4) Security Operations
(a) OUS member institutions have a responsibility to construct operational standards and policies that ensure due care is taken to secure Information Assets. These operational standards and policies should include reasonable and appropriate proactive and reactive measures to protect Information Assets from unauthorized access, disruption of normal operations, and that comply with appropriate laws and regulations. In particular, member institutions should provide anti-virus software, a system to distribute current anti-virus definitions, and a security patch management system for commonly used operating systems.
(b) At a minimum each member institution shall establish:
(A) An incident response plan. This plan shall include a threat containment strategy, an intrusion detection system, and a mechanism for tracking and reporting security breaches.
(B) A notification and escalation plan for security breaches involving personally identifiable information. This plan shall include clearly defined criteria used to determine that personally identifiable information has been exposed and has been, or it is reasonably believed to have been, obtained by an unauthorized person. This plan shall also include clear escalation and notification steps when such an event occurs and the means by which the member institution’s administration, OUS’ administration, appropriate law enforcement agencies, and the people that could be identified by the information in question, are notified of the breach.
(C) An ongoing risk assessment program. This program should regularly identify and track all Essential and/or Highly Sensitive Information Assets, and verify that the appropriate security baseline is in place and being followed with respect to those Information Assets.
(5) Network and Telecommunications Security
(a) OUS member institutions have a responsibility to ensure secure management of their local networks. Member institutions should have the ability to control who connects to their networks, the ability to create secure zones with restricted access on their networks, and be able to ensure the effective operation of their networks.
(b) At a minimum each member institution shall establish:
(A) Secured Zones for Essential and Highly Sensitive Information Assets. These zones shall be created by employing standard network technology to restrict access at the network level to authorized personnel only.

(B) Policies that prohibit transmission of unencrypted Highly Sensitive data outside of secured zones.

(6) Physical and Environmental Security
(a) Each member Institution should establish procedures for the physical protection of its Information Assets. Protection of physical equipment or of software and data residing on storage media, from theft, loss, damage, or improper use should be addressed. Particular attention must be paid where access to or function of Essential or Highly Sensitive Information Assets is concerned; however, member institutions should also consider physical security for computers and other local Information Assets housed in departmental work areas or under departmental control, such as laptop computers, PDAs, etc. Member institutions should adopt policies that only allow Highly Sensitive data to be permanently retained on portable equipment if protective measures, such as encryption, are implemented that safeguard the confidentiality and integrity of the data in the event of theft or loss of the portable equipment.

(b) At a minimum, member institutions shall develop policies and procedures to:
(A) Protect physical areas containing Information Assets that represent Essential or Highly Sensitive information systems that are critical to the functioning of the institution.
(B) Ensure that disposal procedures remove or render sensitive data irretrievable from hard drives, compact disks, external memory, PDAs, etc.
(c) In addition, physical inventories of equipment should be completed and maintained in accordance with section 55.100 of the OUS Fiscal Policy Manual.

(7) Disaster Recovery
(a) As part of ongoing business continuity planning, member institutions are responsible for preparing, periodically updating, and regularly testing a campus Disaster Recovery Plan. This plan should address recovering from a disaster that renders Essential Information Assets unavailable for an unacceptable period of time. Such a Disaster Recovery Plan should establish the frequency of testing member institution disaster recovery procedures. Member institutions should ensure that any local operations procedures are coordinated with overall institutional disaster preparedness plans.

(8) Awareness, Education, and Training
(a) Member institutions are required to develop methods for increasing the level of awareness of information security issues among their constituents. Awareness and training programs may be carried out using a number of different approaches, including document distribution, software distribution, web publishing, and internal or external training sessions. These programs should be carried out on a regular basis and they should be periodically reevaluated in order to assess their effectiveness.

(b) At a minimum, users should be made aware of their roles and responsibilities within the organization as they relate to the security of Information Systems. Users should also be informed of all policies and procedures that may apply to them. Contact information for central IT Security personnel, as well as department IT personnel, should be made available. Users should be informed of whom to contact and appropriate measures to take in the event of a security incident. Policies and procedures should be made readily available in accessible locations.
(c) Educational or training materials should be made available in order to educate users on standard security practices. Training on basic computer security concepts should be provided. These concepts include the following: operating system patching, built-in firewalls, anti-virus software, password management, and browser and e-mail security. Additional training should be offered in areas that are of particular concern to the institution.

Policy Review Process

580-XXX-0050
The OUS CISO will review this policy annually to ensure that it complies with applicable law and Board Policies. Should this policy be revised, the CIOs (or equivalent) of each member institution will be notified to ensure local policies are reviewed and revised as appropriate.

Audit

580-XXX-0060
The OUS Internal Audit office has the authority to conduct periodic information security policy audits using the COBIT framework or suitable substitute to ensure compliance and notify each member institution of any noted deficiencies.

Glossary

580-XXX-0100
(1) Anti-Virus – Programs that identify malicious code installed on computers without the owner/operator’s knowledge or consent.
(2) Applications – Computer programs that collect, process, or otherwise manipulate data.
(3) Best Practice – Generally accepted industry practices that have been broadly adopted and considered standard.
(4) Built-in Firewall – Functions within the local operating system of a computer that limit what other machines on the network can connect to it.
(5) Business Continuity – The ability for business processes and functions to continue and for an organization to continue to function despite emergencies, major disruptions, etc.
(6) CIO – Chief Information Officer. The executive level position in an organization that is generally in charge of the Information Technology division and is responsible for the overall IT operations of an organization.
(7) CISO – Chief Information Security Officer. Generally, the CISO function is one of being responsible for the Information Security Program.
(8) Data – Information stored electronically or in print.
(9) Due Care – The conduct that a reasonable man or woman will exercise in a particular situation in looking out for the safety of others. If one uses due care, then an injured party cannot prove negligence. This is one of those nebulous standards by which negligence is tested. Each juror has to determine what a "reasonable" man or woman would do.
(10) Essential Information Assets – Those Information Assets that are critical to the function of the member institution and without which the normal business functions of the member institution cannot occur.
(11) FERPA – Family Educational Rights Privacy Act. This federal act protects student records, other than directory information, as private information available only to those with an educational need to know.
(12) HIPPA – Health Information Protection and Privacy Act. This federal act protects health records as private information.
(13) Highly Sensitive Information Assets – Those Information Assets that OUS is obligated by law or contract to protect or that represent obviously confidential data that, if released, would represent some actual legal liability to the member institution.
(14) Incident Response – The planned reaction to a breach of security that includes identifying the breach, closing it, and mitigating its effect.
(15) Information Assets – Information and systems that are owned by OUS, information that OUS is obligated to keep secure by applicable law or by contract, and information exempt from disclosure under public records laws. OUS Information Assets are found in written, spoken, electronic, printed, magnetic, optical, and other mediums.
(16) Information Systems – A collection of computers and processes that interact with each other to manipulate, transmit, and store data.
(17) Infrastructure Systems – Computers and network devices and the operating systems that run them.
(18) Institutional Community Members – Faculty, staff, students, vendors, visitors, affiliates, courtesy faculty, etc. In short, all persons who have a relationship with the institution and therefore may interact with Information Assets of the Institution.
(19) Intrusion Detection System – A program or series of programs that watch network traffic and other activities to identify intrusion attempts and compromised machines.
(20) Risk Assessment – In the context of information security, risk assessment is the determination of both the importance of all Information Assets and their likelihood of being accessed by an unauthorized person or of their function being intentionally impaired by someone.
(21) Security Baseline – A minimum set of operational guidelines that affect the relative security of an Information Asset. These guidelines would typically cover such things as firewall settings and network access controls, local permissions, password change policy, operating system patch management, anti-virus policy, and physical access controls.
(22) Security Breach – Theft or unauthorized acquisition of Information Assets by a person that harms or poses an actual threat to the security, confidentiality, or integrity of those assets.
(23) Security Controls – Procedures to follow that help establish and maintain Authentication, Authorization, and Access to Information Assets. These controls include such things as verifying identity, giving access to Information Assets based on job function or duties, network appliances that restrict connections coming from the Internet or unsecured zones, etc.
(24) Threat Containment – Reactive measure to ensure that a security breach is contained to affected systems and that those systems are not able to be used to launch successful intrusion attempts to other systems.
(25) Operating System – The series of programs loaded on a computer that operates it. Common operating systems include Windows, MacOS, and Unix.
(26) OUS Member Institutions – The Chancellor’s Office, Eastern Oregon University, Oregon Institute of Technology, Oregon State University, Portland State University, Southern Oregon University, University of Oregon, and Western Oregon University.
(27) Password Management – The practice of creating and maintaining passwords on a system that are not easily guessed, programmatically determined, or otherwise obtained by
unauthorized persons. This generally means requiring a base level of complexity in the password and that it is changed on a regular basis.

(28) Personally Identifiable Information — A combination of name and one or more other data elements that could uniquely identify an individual for the purpose of providing restricted access. This term may be formally defined shortly in anti “ID Theft” legislation. Common data elements used in combination with name are: Social Security number, driver’s license numbers, date of birth, account number (such as credit or debit card number), account passwords (including pass phrases such as mother’s maiden name), identification number issued by a foreign nation, passport number, biometric data, etc.

**COMMITTEE DISCUSSION:**

Vice Chancellor Kenton introduced John Dolan, Associate Director of Network Services at OSU and Cathy Berg from the Internal Audit Department. Dr. Kenton reminded the Board that an audit was conducted in the spring of 2006 to review information security policies. While campuses were found to have fairly good practices, “they lacked documented policies. Audit staff suggested that policies be developed at the System-level with campus policies developed accordingly.” A subcommittee was formed, which Mr. Dolan chaired, and consisted of IT leaders from OIT, PSU, and the UO.

The Committee reviewed similar policies from private corporations and other educational systems, in particular from the California State System. From this review, the Committee developed and adopted a standard policy framework that was identified in most of the models studied and then tailored it specifically to OUS and the particular conditions here. This framework was studied by the CIOs, records officers of the System, presidents, provosts, and administrative counsels.

An umbrella policy was adopted for the System and then each campus was directed to document and develop, in a case where they were not already developed, policies that would identify and classify critical security-sensitive information. These campus-based policies will be reviewed periodically by the Internal Audit group to ensure that they are comprehensive and complete.

Director Blair questioned the approach of each campus developing a policy and whether or not that was an efficient approach. Ms. Berg indicated that the Committee looked at eight different areas and most institutions already have procedures to accommodate the issues in the policy. However, at this point, the Committee did not test the effectiveness of the campuses' procedures – rather, it was a survey to be sure that they were in place. “What I hear you saying,” Director Blair continued, “is that you think institutions at least have most of the framework they need. Whether they're actually executing against it the way they should be, you're not going to know unless you actually do some testing. That may suggest that we're all right with a broad umbrella, but when are you going to do the audit work?” he asked.

Ms. Berg projected that the audit would be in October or November, at which time the Board could reassess where the institutions are and whether there needs to be some major
overhauling. “I don't think we should be doing that by letting seven different universities go out and figure out seven different strategies or approaches to making the tradeoff,” she continued.

Mr. Dolan reported that the Committee had been working with Oregon's Chief Security Officer. “The funding mechanism for that organization within the Department of Administrative Services is actually an assessment back to departments that rely on those services. There are state services that we would be able to leverage, but they would, in fact, want money out of our pocket to use their resources.”

President Ray indicated that a lot of work has been ongoing at the institution-level. “Probably the one area of vulnerability that I was most concerned about came out of things like the Veterans Administration losing personal data.” This raised, for him, the notion of how to protect information on individual's laptop computers. “I know that many are working on making changes now as they are discovering changes that are vulnerabilities and they're sharing them across campuses,” he added.

It was suggested by Vice Chancellor Kenton that “we move forward with this policy largely as presented; let the audits occur; and continue to review them to keep this front and center and make sure all of the pieces are in place.” Director Blair returned to his broader philosophical point. “We operate in a System where I think our sense is, we'll make it the same where we can, whereas, I think our esthetic ultimately has to be it will be the same unless there is a compelling reason for it to be different. Those are very different mindsets and I think the second ultimately is going to make us a more effective steward of the resources we're given than the first one.”

It was explained that the presentation at this meeting was a first reading of the proposed policy. The next step, with approval of the Board, is to move this proposal as an administrative rule and begin to go through the full process. It should be ready for Board adoption by June. There were questions about where the System and the institutions were in terms of implementation. Mr. Dolan indicated, “For the core administrative systems, this is already done. It's really when we get out into the individual departments, individual researchers within the institution, where the work needs to be done.”

Director Van Vliet cautioned getting an administrative rule approved before there has been sufficient time to be sure it is right because it takes a lot of work to reverse or change a rule. Dr. Kenton responded that the System does not have a policy on these issues at the present time and that first steps need to be taken. “I do think that it will require amendments from time-to-time as technology changes and new issues develop. I do think it is important that we signal the significance and importance of this issue to our community, writ large, which is every faculty member, every staff member, many of our students, our extension offices across the state. It's a big task to educate people.”

4. **ADJOURNMENT**

With no further business offered, Chair Blair adjourned the meeting at 10:15 a.m.