INSTRUCTIONS:
Please review the attached and return to the Office of Procedures, Records, and Forms by the indicated "Respond" date.

<table>
<thead>
<tr>
<th>SECTIONS OR FORM NAME</th>
<th>NUMBER</th>
<th>RESPONSIBLE OFFICIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>WSU Information Security Policy</td>
<td>EPM EP37</td>
<td>Sasi Pillay</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>REVIEWER</th>
<th>RESPONSIBLE OFFICIAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sasi Pillay</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>INFORMATIONAL COPY</th>
<th>TYPE OF CHANGE</th>
<th>RESPONSIBLE OFFICE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tom Ambrosi</td>
<td>New Section</td>
<td>Information Technology Services</td>
</tr>
</tbody>
</table>

DESCRIPTION
This new policy provides requirements for safeguarding the confidentiality, integrity, and availability of institutional data and for the protection of institutional information systems and devices that store, process, or transmit institutional data.

Note to Sasi -- As vice president in charge of administering this policy, it's up to you whether or not to take this proposed new policy to a senior executive administration group (e.g., Senior Staff) and/or the President for review.

Return comments or approval to Deb Bartlett, Procedures, Records, and Forms.

| REVIEWER'S COMMENTS |

The reviewer marks one of the boxes below and signs the form.

- [ ] I concur.
- [ ] I concur in general. See comments.
- [ ] I do not concur. See comments.
- [ ] I defer comments.

| REVIEWER'S SIGNATURE/DATE |

Return to Procedures, Records, and Forms, ITB 3089, mail code 1225.
WSU Information Security Policy

PURPOSE

The purpose of this policy is to establish University requirements for safeguarding the confidentiality, integrity, and availability of institutional data and for the protection of institutional information systems and devices that store, process, or transmit institutional data.

The requirements set forth in this document are based on generally accepted information security principles and form the foundation of the University Information Security Program. This policy is also intended to support the University in:

- Complying with state and federal policies, standards, and regulations (e.g., Family Educational Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPAA), Washington State Office of the Chief Information Officer Policy No. 141);
- Complying with University contractual and data sharing agreements; and
- Achieving its vision and strategic goals in the areas of research, teaching, outreach, and engagement.

SCOPE

This policy applies to all University administrators, faculty, staff, students, affiliates, and third parties who manage or access institutional data or systems that store, process, transmit, or share institutional data.

POLICY

- Washington State University (WSU) must establish a University-wide Information Security and Privacy Program.

- All University information technology assets must be appropriately protected to ensure the confidentiality, integrity, and availability of institutional data throughout its entire life cycle, in a manner that is reasonable and commensurate with:
  - The criticality to the University mission and business operations;
  - The level of confidentiality and privacy of the information content; and
  - Applicable legal and regulatory requirements.

- All users of institutional systems and data must adhere to all applicable University policies, standards, and procedures governing the use of, and access to, institutional data.
WSU Information Security Policy

POLICY (cont.)

• Each University area and college head (e.g., vice presidents, deans, directors) is accountable for ensuring the implementation and monitoring of:
  
  ○ Institutional systems and data under the area's or college's purview for compliance with this policy; and
  
  ○ Other applicable information security and privacy related policies, standards, laws, regulations, and data sharing agreements and/or vendor contracts with third parties.

  A vendor contract review and risk assessment must be conducted prior to WSU releasing or receiving confidential data, to or from a third party.

• Information security awareness education and training must be provided to all University employees that is appropriate for their job classification and information security-related roles and responsibilities.

ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO)

The University official who is accountable for the establishment, implementation, and maintenance of the University-wide Information Security and Privacy Program. The Office of the CIO is authorized to establish, publish, and maintain the information technology, security, and privacy related policies, standards, procedures, and guidelines necessary to ensure the confidentiality, integrity, and availability of institutional data.

Institution-wide, information technology, security, and privacy related policies are developed and approved through established University information technology governance processes.

Enforcement

The Office of the Chief Information Officer is responsible for enforcing this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University or state policies and handbooks (e.g., the WSU Faculty Manual, the Administrative Professional Handbook, WAC 357-40 (civil service employees), applicable collective bargaining agreements, or the WSU Standards of Conduct for Students, WAC 504-26).

Maintenance

This policy is to be reviewed at least annually or on an as-needed basis due to changes to the technology environment, business operations, or regulatory requirements.
WSU Information Security Policy

Exceptions

Exceptions to this policy must be approved by the Office of the CIO, under the guidance of the University Chief Information Security Officer and the President’s Cabinet.

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exceptions. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

DEFINITIONS

Criticality

Criticality is defined as a measure of the importance of the data to the University’s mission and business operations. Data considered confidential may not necessarily be considered critical. Determining the criticality of a particular information system or data set must take into consideration the following:

- What is the impact to the University if the data is not recovered?
- How long will the data recovery process take?
- What is the effect of the loss of the data set during the recovery time, to include potential risks to the University (e.g., information security and privacy, financial, legal, regulatory, reputational, and operational)?

See also Business Policies and Procedures Manual (BPPM) 90.15 regarding essential records protection.

Institutional Data

Institutional data are the items of information, which are collected, maintained, and used for the continued operations of Washington State University, specifically administrative data and other data maintained and safeguarded for University operational purposes. This includes data held by central offices as well as data held by departments or individuals.

Operational data such as that held by the Office of the Vice President for Research support offices (Research Support and Operations (ORSO), Research Assurances (ORA), and Commercialization (OC)), are covered by the data policies in EP8 and EP37. For security and retention rules for such data, contact the Office of Research, the Graduate School, Student Affairs, Enrollment Management, and/or Institutional Research.

Institutional Systems

Institutional systems are defined as the infrastructure, devices, processes, procedures and capabilities that allow the University to manage, store, transmit, process, and share information in pursuit of its mission and business objectives.