WSU Information Security Policy

PURPOSE

The purpose of this policy is to establish the authority to develop a WSU system Information Security and Privacy Program and to establish high-level requirements for:

- Safeguarding the confidentiality, integrity, availability, and privacy of institutional data; and
- The protection of WSU information systems, services, and devices that collect, store, process, share, or transmit institutional data.

The intent of the Information Security and Privacy Program is to define an information security framework appropriate for protecting institutional data and information systems. This policy reflects WSU’s commitment to protect institutional data it creates, collects, stores, processes, shares, and transmits. The requirements set forth in this document are based on generally accepted information security principles to include applicable federal, state, and industry standards. These requirements are to form the foundation of the WSU system Information Security and Privacy Program. This policy is also intended to support WSU in:

- Complying with contractual agreements and applicable state, federal, and industry policies, standards, laws, and regulations;
- Reducing information security and privacy risk exposures; and
- Achieving its mission and strategic goals in the areas of research, teaching, outreach, and engagement.

SCOPE

This policy applies to all WSU business units, workforce members, and information systems, services, and devices that collect, store, process, share, or transmit institutional data.

POLICY

- The Chief Information Officer (CIO) is the WSU official who is accountable for and is authorized to establish and maintain a WSU system Information Security and Privacy Program, and to authorize publication of the information security and privacy related policies, standards, and guidelines necessary to ensure the confidentiality, integrity, and availability of institutional data and systems.
WSU Information Security Policy

POLICY (cont.)

- WSU information systems, services, devices, and data must be appropriately protected to ensure the confidentiality, integrity, availability, and privacy 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 classification of the information; and
  - Applicable legal, regulatory, and contractual requirements.

- Executive heads of major WSU business units (e.g., vice presidents, chancellors, deans) are accountable for the following under their organization's purview:
  - Ensuring compliance with WSU information security and privacy related policies and standards regarding the procurement, implementation, management, and maintenance of organizational business processes, institutional data, and information systems, services, and devices;
  - Compliance with contractual and data sharing agreements with third parties; and
  - Compliance with other applicable information security and privacy related policies, standards, laws, and regulations. (See also BPPM 87.01.)

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

- All users of WSU systems, services, devices, and data are responsible for adhering to all applicable WSU policies, standards, and procedures governing the use and release of, and access to, institutional data.

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

- WSU system information security and privacy-related policies are to be developed and approved through established WSU information technology governance processes (e.g., Information Technology Strategic Advisory Committee). (See also BPPM 87.01.)
WSU Information Security Policy

Enforcement

The Office of the CIO is responsible and has the authority for enforcing compliance with this policy.

Violations

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable WSU 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

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, or legal or regulatory requirements.

Exceptions

Exceptions to this policy must be approved by the Office of the CIO, under the guidance of the appropriate information owner(s) and the University Chief Information Security Officer.

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.

Related Information

See BPPM 87.01: Information Security Roles, Responsibilities, and Definitions.