WSU Information Technology Services Review

Faculty Senate 11.03.22

Sasi Pillay, Vice President & Chief Information Officer

Michael Walters, Assistant Vice President & Chief Information Security Officer

Tony Opheim, Associate Vice President & Deputy Chief Information Officer

Relevant Information Security Policies

- EP8: WSU Data Policy (February 2022)
  - Establishes data administration policy, roles and responsibilities, classification of data
- EP37: WSU Information Security Policy (August 2022)
  - Defines information security framework and compliance requirement
- BPPM 87.20: Security Assessment and Authorization (July 2020)
  - Establishes requirement for conducting security assessments
- BPPM 87.55: Information Security Incident Management and Breach Notification (March 2022)
  - Establishes requirement for reporting and responding to security incidents

EP8 - WSU System Data Policies

Identifies five key areas which require data policy statements:

- Data Administration - Management accountability for administering institutional data
- Data Authorization and Access - Authorization and access to institutional data
- Data Usage - Appropriate use and release of institutional data
- Data Maintenance - Upkeep of institutional data
- Data Security - Protection of WSU system information systems, services, devices, and data

Defines information classification categories:

- Public - Does not need protection from unauthorized access or disclosure
- WSU Internal - Release must be approved by the Information Owner
- Confidential - Unauthorized access or disclosure could cause significant harm to WSU
- Regulated - Unauthorized access may cause serious reputational, legal, financial consequences

EP37 - WSU Information Security Policy

Security Awareness Training - all employees are required to complete cyber security training within six months of:

- The effective date of the revision to EP37 that adds the cyber security training requirement (Jan. 31, 2023); or
- The date of hire, if hired after the effective revision date
- Available at HRS Skillsoft Percipio (https://wsu.percipio.com/)

BPPM 87.20 - Security Assessment and Authorization

An Information Owner is an executive head of a major WSU system business unit (e.g., vice president, chancellor, or dean)

- Is accountable for the stewardship of institutional data within their area of responsibility
- Is responsible for ensuring the information security and privacy of institutional data
- May delegate these administrative duties to one or more WSU system administrators known as data custodians for specific institutional data sets or functional areas
- Explicitly accepting the risk of information systems based on the implementation of an established set of security controls

Information Technology Services has developed processes for security and risk assessments to determine gaps in security control objectives and identification of associated risks.

BPPM 87.55 - Incident Response and Breach Notification

Establishes a consistent and coordinated approach to handling security incidents:

- All information security incidents are to be reported as soon as it is practicable after discovery
- Various state and federal laws and regulations may contain specific incident and/or breach reporting requirements
- All information security incidents involving an unauthorized or potential disclosure, loss, theft, or misuse of WSU confidential and/or regulated information are to be escalated immediately after discovery to the CISO, the CCRO, and the applicable delegated authority

Information owners are accountable for appropriately responding to information security incidents that may adversely affect the confidentiality, integrity, and/or availability of institutional systems, services, and data under their care, as required by institutional policies and all applicable laws and regulations.

Email Risk Management

- Recent ITS Improvements:
  - Multi-Factor Authentication
  - Server-to-Server Email Authentication
  - External Email Warning

- Individual Email Policy
  - Draft currently being circulated for review
  - Requires an exception to allow staff and faculty to automatically forward all email to non-WSU email systems
  - Sending individual emails that do not contain restricted information is acceptable
  - NOTE: Forwarded emails to personal email addresses (i.e., Gmail, Yahoo, Outlook.com) are still subject to public records requests

Mobile Device Risk Management

- Recent ITS Improvements:
  - Endpoint Security Standards updated (https://its.wsu.edu/documents/2022/02/wsu-endpoint-security-standard-v1-2-2022.pdf)
  - Implemented two Mobile Device Management Platforms (InTune & Jamf) to cover all mobile device operating systems (PC, Mac, Android, and iOS)

- Top actions faculty can take to help minimize risk to WSU:
  - Register university laptops, tablets, and cell phones with unit Device Management Platform (i.e., Intune or Jamf)
  - Encrypt all hard drives (both internal and external/USB)
  - Synchronize (backup) important documents and data to OneDrive
  - Install ITS supported security agent (Cortex XDR)
  - Protect device with strong password or passcode

WSU Information Technology Services (ITS)

- Thank you for the opportunity to connect with Faculty Senate.