Data Security and User Responsibilities

How to Contribute to WSU’s IT Security Posture
Introduction

Information Technology Services (ITS) / Information Security Services (ISS)

Keela Ruppenthal
GRC Team (Governance, Risk, and Compliance)
Where to Find Guidance

WSU Administrative Manuals

https://policies.wsu.edu/prf/index/manuals/

Business Policies and Procedures (BPPM)

Guidance for university employees and administrators

Based upon approved University administrative policies and applicable state and/or federal statutes and regulations

Executive Policy (EP)

University system policies are approved by the appropriate governing body of University executive officers

Cover a variety of topics related to the WSU system
BPPM Policies

Chapter 87
Specific to Information Security
Managed by ISS
Catalog is Actively Growing

Chapter 88
Related to Information Privacy
Not managed by ISS
Important Information for Healthcare Data

Chapter 90
Retention Schedule for University Records
Not managed by ISS
Executive Policy Manual

- EP04 – Electronic Communication Policy
  - Governs appropriate use of WSU Information Technology (IT) resources

- EP08 – WSU System Data Policies
  - Data Administration
  - Data Authorization and Access
  - Data Usage
  - Data Maintenance
  - Data Security

  - High-level requirements about safeguarding confidentiality, integrity, availability, and privacy of institutional data

EP Policy Links


User Responsibilities EP8

Follow WSU policies, standards, procedures, and guidelines
Report suspected or actual vulnerabilities
Roles & Responsibilities

BPPM 87.01 - WSU Information Security Roles, Responsibilities, and Definitions

https://policies.wsu.edu/prf/index/manuals/business-policies-and-procedures-manual/bppm-87-01/

Information security roles, responsibilities, and definitions enable effective communications

   Aligns and Defines Expectations

A common lexicon forms a common understanding and ensures consistency
Data Classification

EPo8 – WSU System Data Policies


• Not all data requires the same level of security controls
  • Proper classification ensures data is safeguarded with the necessary measures
• Various regulations and data protection laws mandate the protection and appropriate handling of sensitive data.
• Least Privilege
Regulated WSU Data Types

- **Student Data**
  - Family Educational Rights and Privacy Act (FERPA)
- **Payment Card Industry (PCI)**
  - Payment Card Industry Data Security Standard (PCI DSS)
- **Electronic protected health information (ePHI)**
  - Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- **Financial Data**
  - Gramm-Leach-Bliley Act (GLBA)

This list is not comprehensive.
Cloud Services

Cloud Cliché:
“There is no Cloud, It’s just someone else’s computer.”

Recommend using WSU System Enterprise Services

Cloud providers are required to adhere to the same WSU Policy requirements.

If a service is not listed on the matrix, the vendor will need an IT Security review.

WSU Cloud Acceptable Use Matrix

<table>
<thead>
<tr>
<th>WSU Service</th>
<th>Public</th>
<th>Human Subjects - Identified</th>
<th>Internal</th>
<th>Student Education Records (FERPA)</th>
<th>Personal Information (RCW 42.56.390)</th>
<th>Human Subjects Identifiable (Non-Regulated)</th>
<th>Student Loan Application Data (GLBA)</th>
<th>Protected Health Information (HIPAA)*</th>
<th>Payment Card Information (PCI)</th>
<th>Export Controlled Research (ITAR/EAR)</th>
<th>Federal Information Security Management Act (FISMA)</th>
<th>EU General Data Protection Regulation (GDPR)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office 365 Email</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>*</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Zoom</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>*</td>
<td>*</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>OneDrive</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>*</td>
<td>*</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Teams - Modern Groups/Sites</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Qualtrics</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>*</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
<tr>
<td>Redcap</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>*</td>
<td>*</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
<td>⬤</td>
</tr>
</tbody>
</table>

https://its.wsu.edu/information-security/wsu-cloud-acceptable-use-matrix/
Reporting Security Incidents

Contact Information
WSU Pullman Information Technology Services (ITS)–Security Operations Center
Email: abuse@wsu.edu
Telephone: 509-335-0404

Security Incidents are to be reported as soon reasonably possible after discovery
By secure electronic means (e.g., internal WSU Office365 e-mail services)
Non-WSU information systems such as commercial e-mail services (e.g., gmail) are not to be used

WSU Confidential and/or Regulated information incidents are to be escalated immediately after discovery
To: WSU Chief Information Security Officer (CISO)
WSU Chief Compliance and Risk Officer (CCRO)
Applicable delegated authority.

State/Federal laws and regulations may contain specific incident and/or breach reporting requirements
Understand your data and the specific reporting requirements

What is an incident?
Information Security Incident = Unauthorized or Potential Disclosure, Loss, Theft, or Misuse of institutional data

BPPM Policy Link
Crimson Service Desk

https://its.wsu.edu/csd/