Revision of
The WPI Acceptable Use Policy

7th Faculty Meeting of AY 2021-22

March 17, 2022

Background

- The Acceptable Use Policy (AUP) governs the use of all WPI IT resources by all WPI community members.
  - Everyone at WPI is expected to read, understand, and adhere to the AUP.
- The AUP was last revised and updated in 2015.
  - Collaboratively written and approved by IT and CITP.
- ITS brought to CITP an updated policy.
  - Revisions are mainly to formatting and sectioning in accordance with new OGC template; some terminology is revised.
  - All key elements of the policy remain the same.
  - Among the purposes of this discussion: raise awareness / refresh memories about the AUP.

Scope and Definitions

- "Users" : all members of the WPI community authorized to access WPI Computing and Networking Resources.
- "WPI Computing and Networking Resources"
  - Systems, networks, applications, information, lab computers, research computers, and similar owned by WPI.
  - WPI computing and networking resources that are accessed by personally-owned devices (such as a personal mobile device).

- **Revisions:** more specific language.

This policy applies to all users of WPI technology resources. It applies to any systems, software, components, or data that are connected to or utilize the WPI network and its computer systems. It applies to both academic and non-academic communication and activities.

Policy: Five Key Elements

1. Comply with the intended use of WPI C&N Resources.
   - Academic and campus business use are primary; non-academic use is secondary.
   - Users shall comply with technical, administrative, and process controls.
   - Users shall not engage in disruptive activity or subvert a system for illegal or inappropriate use.
2. Ensure the ethical and legal use of WPI C&N Resources.
   - Shall respect privacy of others; shall not harass or attack others; shall abide by federal, state, and local laws.
3. Respect WPI property and WPI C&N Resources.
   - Shall not bypass technical controls or grant access to individuals outside WPI w/o permission from CISO/CIO.
   - Know that WPI has certain rights regarding its operation of C&N Resources.

Policy: Five Key Elements

4. Respect the personal property and privacy of other users.
   - Refrain from monitoring / accessing private information without permission.
   - Respect copyright regulations and personal copyright of others.

5. Use the WPI C&N Resources for non-commercial purposes only.
   - Shall not use for commercial purposes, or to host advertising, or to create/mine digital currencies.
   - Shall not resell C&N Resources.

- **Revisions:** minor editing. These five key elements are the same as existing policy.

University Response to AUP Violations

- First and/or Minor Violations
  - Non-adversarial and educational conversation with Information Security.
- Repeat Violations
  - Students may be referred to Dean of Students Office, and C&N resources disabled for up to one week. Employees may be referred to T&I.
- Serious Violations: that exhibit malicious intent to compromise or circumvent security of C&N resources
  - Students: will be referred to Dean of Students Office, and C&N resources suspended pending resolution. Employees: referred to T&I.

University Response to AUP Violations

- **Revisions:**
  - Nature of responses to violations remains the same.
  - "Violations" instead of "Offenses."
  - Clearer distinctions between Student/Employee and Repeat/Serious.
  - Slightly lesser detail for response to Repeat Violations.

Repeat and/or Serious Offenses: In the event of suspected repeat offenses, students will have a meeting with a member of Information Security to discuss the further offenses. During the meeting, the alleged violations and the AUP policy will be reviewed. If the student admits responsibility for the violations, they will sign an AUP Administrative Agreement. As part of the resolution to the incident, computers and resources that are registered to the individual may be disabled for up to one week following this meeting. The AUP Administrative Agreement and supporting documentation will be filed with the Dean of Students Office and a formal judicial record will be created. If the student does not admit responsibility for the alleged violation, the case will be forwarded to the Dean of Students Office for resolution.

Exceptions to the AUP

- Granted on a case-by-case basis by Information Security.
- Exceptions for academic purposes can be requested by a Faculty member.
- **Revisions:** minor editing.