Network Security Policy

I. Policy Statement

WPI recognizes the importance of simultaneously supporting open, unrestricted network access expected in a diverse academic environment while also protecting sensitive information from unauthorized access. This policy establishes technologies and protocols in protecting WPI's network and information from unauthorized access, attack, or damage.

II. Scope

This policy applies to devices connected to the WPI network and the WPI students, faculty, staff, administrators, trustees, contractors, vendors, and any other individuals who use these devices while they access the WPI Network.

III. Definitions

"WPI Network" means all WPI-owned or operated wired and wireless communications equipment, including all physical networking infrastructure, cabling, routers, switches, and wireless access points, firewalls and other network protection devices, load balancers, communication links to cloud providers and ISPs, enabling services including DHCP, DNS, and RADIUS servers, cellular, VoIP and cable TV.

"Computer System Hardware" means any computer device or hardware that connects to the WPI network, whether owned by WPI or personally owned, including without limitation desktops, laptops, smartphones, or tablets.

"Passive Security Monitoring" is a type of security solution that automates security monitoring across various sources of security information. This type of monitoring provides real-time visibility into an organization's security posture, constantly monitoring for cyber threats, security misconfigurations, or other vulnerabilities by monitoring network traffic. Passive Security monitoring does not scan individual computer devices.

IV. Policy

A. Roles and Responsibilities

1. WPI Information Technology Services (ITS) has primary responsibility for (i) implementing, maintaining, securing, and supporting the WPI Network, and (ii) mitigating risks associated with the unauthorized access to, disclosure of, loss, or theft of information on the WPI Network.

2. WPI ITS is responsible for ensuring that all Computer System Hardware connected to the WPI Network or the WPI Research Computing subnetwork meets all WPI ITS security requirements.

3. For Computer System Hardware that is not on the WPI domain (admin.wpi.edu), the device owner is responsible for ensuring that operating systems and antivirus applications are installed, enabled, and remain current.

4. As the network operator, WPI ITS may deny access to the WPI Network to any Computer System Hardware that poses a threat to the network, such as a machine infected with a virus or malware.

5. As the network operator, WPI ITS may conduct Passive Security Monitoring on any Computer System Hardware connected to the WPI Network. Passive Security Monitoring provides a means by which to confirm that information resource security controls are in place, effective and are not being bypassed. One of the benefits of security monitoring is the early identification of wrongdoing or new security vulnerabilities, which can prevent possible attacks or minimize their impact on computer systems.

6. WPI does not routinely monitor the content of information transmitted through, or stored in, WPI Systems. For information regarding what type of information WPI may access, please review the Access to User Electronic Information Policy.

B. Security and System Management for Individuals Accessing Restricted Use Data

As indicated in WPI's Data Classification and Usage Policy, certain data that WPI maintains is particularly sensitive. This data, called Restricted Use Data, primarily relates to government identification, financial data, healthcare data, biometrics, and sensitive research affected by export control policies or with military applications. Due to the laws and regulations surrounding this data, additional security and system management measures are required when working with this data, as described below.

1. **Network Segmentation Management.** WPI ITS may require that WPI individuals who have access to Restricted Use Data use a secure segment of the WPI network to access this data.

2. **Approved Remote Access.** Remote access to Restricted Use Data hosted on the WPI Network will only be available for off-site remote access through a centrally-managed VPN system to ensure authenticity and confidential communication. To access Restricted Use Data hosted in cloud-based applications, users will be required to use multi-factor authentication.

3. **Data Loss Prevention.** Data loss prevention (DLP) tools can help prevent the accidental exposure of Restricted Use Data by applying business rules to classify and protect

Restricted Use Data. WPI uses DLP rules in Office 365 to prevent Restricted Use Data from being sent via email. For additional security, WPI ITS encrypts all emails sent within the WPI domain. Individuals who must send Restricted Use Data outside of the WPI domain must work with WPI ITS to ensure messages are encrypted. To comply with state law (201 CMR 17), WPI must protect all Social Security numbers and credit card numbers. For faculty that don't have access to Restricted Use Data, ITS is committed to support a one-time self-service audit and reporting process instead of the automated scanning process. For all other employees that routinely handle Restricted Use Data, ITS

will perform automated scans on WPI-owned computers to locate and protect any such data.

4. **Permitted Systems for Accessing Restricted Use Data.** Due to the sensitivity of Restricted Use Data, only WPI-managed Computer Systems Hardware is permitted to access Restricted Use Data.

C. Exceptions

For any student, faculty or staff member that requires an exception to this policy, please contact WPI's Chief Information Security Officer. All requests for exceptions to this policy will be considered on a case-by-case basis.

V. Questions

For questions about this policy, please send an email to its@wpi.edu.

* * *

Policy Sponsor: Chief Information Officer
Responsible Department: Information Technology
Effective Date (i.e., date of Presidential Approval): September 18, 2020
Revision Date: N/A