Email Whitelisting Policy

1.0 Purpose

The purpose of this policy is to provide guidance on how and when a Trusted Partner email system will be added to Approved Safe Sender Whitelist.

WPI uses email spam filtering tools on the University's email system to block millions of unwanted inbound emails, also known as Junk Mail, SPAM or Phishing Email. However, these spam filtering tools can block some legitimate emails from reaching University inboxes.

To help ensure proper delivery of emails to WPI Inboxes from known trusted parties, Information Technology Services (ITS) maintains an Approved Safe Sender Whitelist.

It should be noted that whitelisting introduces additional cybersecurity risks. Spammers can take advantage of whitelisting, which makes our WPI inboxes more susceptible to spam, phishing scams, and viruses. Whitelisting should only be considered for truly Trusted Partners.

2.0 Definitions

Approved Safe Sender Whitelist - is a list of email addresses, domains, and IP addresses which will not be blocked by WPI's spam filters.

Trusted Partners - Hosted third-party vendors that have a contractual relationship with WPI that send email to students, employees or other university constituents.

3.0 Applicability

This policy applies to all members of the WPI community, including students, faculty, staff, trusted partners, contractors, and users of the university network and messaging systems.

4.0 Policy

The University will place Trusted Partners on the Approved Safe Sender Whitelist if they fall into following criteria:

- Companies that provide benefits to employees.
- Companies that communicate to faculty, staff, and/or students in multiple departments.

- Companies that WPI has grants with in excess of $1 million.
- Companies that WPI has a research relationship with (i.e. UMass).
- Organizations or agencies that communicate regulatory or compliance notices or updates.

5.0 Policy Enforcement

Any person that violates any of the policies found in this policy will be subject to the same disciplinary actions as outlined in WPI's Confidentiality Agreement for employees or Code of Conduct for students. Third-party vendors who violate this policy may have their email messages filtered and their contracts with the university re-evaluated.

6.0 Approval and Revisions

Policy Category: Institutional Risk & Compliance

Policy Approved By: Approved by WPI's Information Security, Risk and Compliance Committee on January 10, 2019.

Policy Reviewed Annually By: Chief Information Security Officer

Last Modified: 1/10/19