University Staff Senate Meeting Agenda

Date: Wednesday, April 8, 2026

Location: Meadowlark Room, Overman Student Center, Pittsburg State University

Time: 1:30 PM

I. Call to Order
II. Roll Call and Confirmation of Quorum
III. Approval of Previous Meeting Minutes
IV. Guest Speaker: Amanda Williams
V. Shared Governance Report
    a. Faculty Senate
    b. Student Government: see April minutes
    c. University Leadership: Emily McElwain
VI. Human Resources Report
    a. General Report
    b. Orientation Report: see March minutes
    c. Employee Initiative Teams (EIT)
        i. Kudos/Recognition
        ii. Professional Development
        iii. Onboarding/Offboarding
        iv. Employee Wellness
        v. Performance Management
VII. Cabinet Update
    a. Presidents' Report
        i. Regents Universities Meeting: see April minutes
        ii. PSU Leadership Meeting: see April minutes
    b. Treasurer's Report: Libby Graham: see April minutes
VIII. Committee Reports
    a. Satisfaction Survey: Michael Woodrum
    b. Parking Committee: Stephanie Willis & Heather Busch
    c. Board of Governors: Donna Jacobs
    d. Display Case Subcommittee: Sarah Moon
    e. Elections Committee: Tracey Eagon
        i. Review election assignments
    f. Bylaws Committee: Tom Smith
        i. Vote on revision
IX. Old Business:
    a. Ribbons for University nametags
    b. End-of-year banquet
X. New Business and Questions
    a. Open to the floor
    b. Next meeting: Wednesday, April 8, 2026, in the Meadowlark Room, Overman Student Center
XI. Adjournment

IT Security Travel Policy

Applies To

This policy applies to Pittsburg State University (PSU) faculty, staff, adjunct, auxiliary, and emeritus who are traveling on behalf of PSU and using or accessing PSU technology resources and/or data while traveling. This group is referred to as "employee(s)" for the purpose of this policy.

Policy Statement

This policy is to ensure the security of PSU data and systems when employees travel for work-related purposes. PSU aims to mitigate potential risks associated with travel, such as data exposure, device loss, credential compromise and unauthorized access to university systems. Employee must take appropriate precautions to safeguard university data.

This policy also ensures that employees are fully aware of their responsibilities and any potential limitations with university systems while traveling. It serves to confirm that they understand the necessary preparations required prior to travel.

Security Requirements

- Review the U.S. Department of state website for travel advisories and destination specific guidance.
- Travel requests should be received **30 days prior to departure.**
    - Submit a ticket to support@pittstate.edu
- Technology Licensing Requirements
    - Adjunct, emeritus, and auxiliary employees must verify that all required software and technology licenses are in place at least 30 days prior to departure**.**
        - Submit a ticket to support@pittstate.edu.
        - Visit the Microsoft Office 365 website for additional information regarding Microsoft licensing requirements.
- Data Security Requirements
    - Travel only with data necessary for the specific work being performed.
        - Sensitive data should be removed or minimized prior to travel
    - Full disk encryption enabled
    - Current OS and security patches applied
    - PSU-approved endpoint protection installed and validated
    - VPN configuration tested
    - Request a Duo bypass code and/or Duo Token from the Gorilla Geeks before departure
    - Change your password before you leave to avoid password expiration while traveling
    - PSU systems should not be accessed from public/shared computers
    - Incident Reporting

        - Report lost, stolen, confiscated devices within 24 hours to the IT Security Officer – itsecurity@pittstate.edu
        - Reset your password immediately if you suspect account compromise
- Travel to Elevated-Risk Locations
    - Review applicable foreign travel advisories and take additional precautions.
    - Contact ITS **30 days prior to departure** to schedule a pre-travel consultation to review specific security guidelines. These may include, but are not limited to:
        - Using a loaner computer that will be reimaged upon return (dept provided)
        - Using a third-party VPN (dept provided)
        - Traveling with a burner phone (dept provided)
        - Do not reuse USB drives that have been connected to international computers
        - Do not connect the computer to the PSU network upon return to the US
        - Returning the computer to ITS for reimaging
- Post-Travel Requirements
    - Change all university passwords and/or PINS
    - Return loaner devices to the Gorilla Geeks for check in and reimaging within five business days of return

Related Information: Travel Guidelines
Contact:
Review Cycle: Annual
Keywords:

Change History:
Created: 6/2025
Updated: 2/2026