University of Pittsburgh Federated Authorization Security Contacts

Overview

This document outlines the criteria for identifying and designating a Federated Authorization Security Contact according to the University's Federated Authorization Process guidelines. Each University area should designate a primary and secondary Security Contact. This document covers:

A. The responsibilities of a Security Contact
B. The qualifications for a Security Contact
C. How to designate a Security Contact
D. How to request that responsibility be removed from a Security Contact

If you have any questions about this procedure, please contact the 24/7 IT Help Desk at 412-624-HELP (4357) or helpdesk@pitt.edu.

A. Security Contact Responsibilities

Security Contacts are responsible for ensuring that only authorized University employees have access to the Student Information Systems (PeopleSoft) and Student Mart data needed to do their jobs. Security Contacts therefore have the important responsibility of preserving student confidentiality and data integrity. As a result, all PeopleSoft and Student Mart user access requests must be reviewed and approved by the Security Contacts. Individuals fulfilling the role of Security Contact must meet certain qualifications in order to ascertain that a user's request is appropriate and to ensure the Federated Authorization process is successfully followed.

B. Security Contact Qualifications

Designated Security Contacts must:

- Understand their University area's business and academic processes
- Be familiar with the job duties of all Student Mart and PeopleSoft users in their area
- Be in a position of authority to independently grant and revoke access privileges
- Complete the appropriate Federated Authorization training course

Note: Security Contacts should have worked with the University Area for several years, giving them an inherent understanding of their area's employees and processes. Therefore, administrative assistants, student workers, new hires, contractors, graduate, and post doc students working in the area would not be the most appropriate choice.

C. Designating a New Security Contact

1. **The head of each University area** (dean, director, regional president, or department head, depending on the University area) should identify a candidate that meets the qualifications above and submit an online request to the attention of the Chief Information Security Officer, identifying the individual and why they were selected. Please include the following information:

    - Security Contact's Name
    - Security Contact's Title
    - Phone number
    - Username
    - Brief description of how the individual meets the criteria for a Security Contact

2. **The Chief Information Security Officer (CISO)** will receive the request from the Pitt IT Help Desk. The CISO then approves or denies the request and notifies the requestor.
   If approved, the CISO notifies the Pitt IT Security team of the new Security Contact to process the next steps.
3. **Pitt IT Security** adds the new Security contact to the relevant Central Directory Service (CDS) group, adds the SA_VIEW_SECURITY_CONTACTS role to their PeopleSoft user profile, and updates the Federated Authorization Security Contact list on the Technology website.
4. **The new Security Contact** completes Federated Authorization Request training.

D. Process for Removing a Security Contact

The head of a University area (dean, director, regional president, or department head, depending on the University area) should **immediately** contact the 24/7 IT Help Desk at 412-624-HELP (4357) or helpdesk@pitt.edu to have a Security Contact removed from the list.

Get Help

The 24/7 IT Help Desk at 412 624-HELP (4357) is available 24-hours a day, seven days a week to answer your technology-related questions. Questions can also be submitted via the Web at technology.pitt.edu.