University of Oregon

Red Flags Team

Charter

July 2020

Mission Statement

The Red Flags Team serves as an advisory group to the Vice President for Finance and Administration and Chief Financial Officer (VPFA/CFO) on administration of the UO Identity Theft Prevention Program (ITPP). VPFA/CFO has authority to make decisions regarding the program. The ITPP program coordinator will report university identity theft and remediation recommendations annually to VPFA/CFO and to the Strategic Enterprise Risk Management and Compliance (SERMC) committee.

The mission of the ITP is to reduce the risk of identity theft and maintain compliance with the FTC Red Flags Rule.

To fulfill this mission the Red Flags Team will create and maintain the UO ITPP, maintain an Identity Theft Prevention training course, and oversee the activities of the ITPP coordinator.

Responsibilities of the team

- Meet semi-annually;
- Review and update the UO ITPP document and fiscal procedure;
- Review the annual status report prepared by the program administrator;
- Prioritize identified risks, and recommend new ITPUs and detection procedures;
- Oversee the campus ITPP training program
- Plan and prioritize risk reduction and compliance remediation activities;
- Identify resources for Red Flags compliance initiatives.
- Provide identity theft assessment for cyber insurance

Membership

The Red Flags Team includes representatives from BAO and other units who's activities and service confer a high risk of identity theft.

Program Coordinator and Team Lead:

The Vice President of Finance and Administration delegated authority to administer the ITPP to the Director, BAO Information Systems

Members

Representatives from:

- BAO Financial Services
- BAO Student Financial Services
- BAO Payroll
- Information Security Office
- Registrar
- ID Card Office
- Health Center
- Financial Aid

Alignment and connection to other campus teams

University of Oregon
Red Flags Team
Charter

The Red Flags Team is connected to other important response and prevention teams on campus through liaison connections and joint membership. These teams include but are not limited to the following:

- The Strategic Enterprise Risk Management and Compliance (SERMC) committee use two approaches to address current or emerging risks that do not have a clearly defined university risk owner.
    - Standing committees and teams to monitor, mitigate, and respond to risk and vulnerabilities, and
    - Workgroups with specially charged workgroups

  The ITPP program coordinator will present the campus report on identity theft annually to SERMC each spring.

- UO Incident Management Team (IMT) – Provides the command and control infrastructure that is required to manage the logistical, fiscal, planning, operation, safety and campus issues related to any and all incidents/emergencies.

- Campus Vulnerability Assessment Team (CVAT) – A collaborative interdisciplinary effort that conducts site specific assessments to identify the vulnerability of people, property, operations and environment.

- Data Security Incident Response Team (DSIRT) – Responsible for reducing the risk associated with data security issues and overseeing the response to data security incidents.

- Information Security and Policy Governance Committee (ISP GC) – Represents subsets of business, research, and teaching technologies, takes recommendations and advice from service advisory boards, and addresses questions about security and information assurance. The UO Chief Information Security Officer is a member of the PCIT providing linkage to the ISP GC.