University of Oregon
Payment Card Industry Team (PCIT)
Charter
July 9, 2015

Mission Statement
The mission of the Payment Card Industry Team (PCIT) is to reduce the risk of card data breach and maintain compliance with Payment Card Industry data security standards.

The PCIT will achieve this mission by maintaining and enforcing the UO Payment Card Acceptance Policy, overseeing the annual PCI risk assessment, engaging a Qualified Security Assessor (QSA), and partnering with campus merchants, business, IT and procurement professionals to ensure university and third party card processing activities are secure and compliant.

Responsibilities of the team include
- Conduct member meeting at least quarterly;
- Maintain UO Payment Card Acceptance Policy;
- Oversee annual attestation of compliance to acquiring bank and notify university leadership regarding compliance status;
- Oversee annual PCI risk assessment performed by the CISO and Internal Audit;
- Oversee consulting engagements with QSA firms;
- Plan and prioritize risk reduction and PCI compliance activities;
- Coordinate resources for campus wide PCI compliance activities.

Membership
The PCIT includes senior leadership representatives from units across the University with expertise in PCI compliance, information technology, information security, risk assessment, business and card operations.

Team Lead:
Director, BAO Information Systems

Members
Chief Information Security Officer Information Services
Chief Auditor Internal Audit
Chief Procurement Officer Purchasing and Contracting

Representatives from:
- IS Security Team
- Enterprise Risk Services
- Intercollegiate Athletics
- Student Life
- Parking and Transportation
- Police Department
- University Advancement
- University Housing/Food Services
Alignment and connection to other campus teams

Additionally, the PCIT 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:

- **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.

- **Other**