California University of Pennsylvania
Pennsylvania State System of Higher Education

Technology Policy Number 2013-01
UTech Security Incident Reporting and Response Policy

Approved by:	**Cabinet**
History:	**Issued -- 1/29/2013**
	Revised --
	Additional History
Related Policies:	
Additional References:	**PASSHE Information Technology Security Guidelines Number 2010-04**

I. Introduction

This policy serves to minimize the negative consequences of an Information Security incident (as defined below) and to improve the University's ability to promptly restore operations affected by such incidents. The University's goal is to assure that incidents are promptly reported to the appropriate University officials, that they are consistently and expertly responded to, and that serious incidents are properly monitored.

II. Purpose

The purpose of information security incident response is:

- To ensure that incidents are promptly reported to the appropriate University officials.
- To mitigate the effects caused by such an incident.
- To protect the information resources of the University from future unauthorized access, use or damage
- Ensure that California University of Pennsylvania fulfills all of its obligations under University policy, and federal and state laws and regulations with respect to such incident.

III. Statement of Policy

- **Who should report a security incident?** Any person (faculty, staff, and student) who knows or reasonably believes that a Security Incident involving a California University

of Pennsylvania-owned Technology Asset has occurred. If it is unclear as to whether a situation should be considered a Security Incident, it should be reported so that University Technology Services can evaluate the situation.

- **How do you report a security incident?** Security incidents must be reported as soon as possible by calling our Helpdesk at 724-938-5911 or by emailing utechrequests@calu.edu. Please be as detailed as possible.

  Anyone who discovers a weakness or vulnerability in the information security measures used by California University of Pennsylvania must not discuss these matters with anyone other than the UTech CARS Team.

- **Response** – Once reported, the University Technology Services Compliance, Auditing, Risk, and Security (CARS) Team will investigate, assess, and respond to threats to California University of Pennsylvania IT resources.

  In cases of lost or stolen University Information Technology (IT) Assets, PASSHE Information Technology Security Guidelines Number 2010-04 - Guidelines on Breach Notification will be followed. Incidents may also be reported to the appropriate law enforcement, PASSHE, or University officials. The UTech CARS Team will handle these notifications.

  Any University information technology assets or personally owned technologies that pose a security threat may be disconnected from the network. If a security breach is discovered in progress, the Incident Response Team may take immediate actions to isolate and deny access to the user, data or information technology asset.

IV. Definitions

- **Information Technology Asset** - A system or systems comprised of computer hardware, software, networking equipment, and any data on these systems. Such assets include but are not necessarily limited to desktop computers, servers, printers, telephones, network equipment, E-mail and web based services.

- **Security Incident** – an incident meeting one or more of the following conditions:
  - A breach, attempted breach or other Unauthorized Access of a California University of Pennsylvania Information Technology Asset. The incident may originate from the California University of Pennsylvania network or an outside entity.
  - Any Internet worms or viruses.
  - Disruption of information technology service levels.
  - Theft or loss of a laptop, desktop, PDA or other electronic device that may contain confidential or sensitive data.
  - Web site defacement.
  - Compromised password(s).
  - Unauthorized use of an individual's computing account.

- Any activity that harms or represents a serious threat to the whole or part of California University of Pennsylvania's computer, telephone and network-based resources.