UNIVERSITY OF Cincinnati Clermont College	*Procedure/Guideline Title:* **Vulnerability Reporting and Remediation**	*Number:* **034.TS.204**
Category: Information Technology	**Effective Date:** 11.16.2016 **Prior Effective Date:**	**Owner:** Technology Steering Committee **Responsible Office(s):** Technology Services
Applicable for: Technology Services	**Enabling Act:** Technology Steering Committee Approval	

Background

As an institution of higher learning, UC Clermont both uses information technology and supplies it to the members of the university community. This procedure has been developed to create a framework that ensures a secure technology environment for all faculty, staff, students and visitors at the college. The primary directive of technology at UC Clermont is to support, promote and enhance the learning process.

As per the University of Cincinnati's policy on Information Technology, all operating units that use information technology shall be responsible for:

- Developing and implementing, when appropriate, additional IT policies, guidelines or procedures specific to their academic or administrative units.

Procedure

Awareness of the proper means of reporting and remediating network vulnerabilities is critical to the overall success of maintaining a secure computing environment. It is the responsibility of the Technology Services staff to follow the outlined procedure.

- Core Services staff generates and reviews scan reports monthly to identify catastrophic and critical vulnerabilities.

- Monthly report/scan are currently placed in Technology Services share, with the intent to move them to the Technology Services Team SharePoint site.

- Based on support areas, i.e. client computing, servers, network hardware, etc., vulnerabilities are grouped together for remediation and appropriately assigned via the Campus Support Desk support call system. Entry oversight is performed by the Core Services Director.

- Remediation is expected to be complete on any assigned items within 30 days.

- If an item cannot be fully remediated by the assigned Technology Services team member, it should be escalated within the original support ticket in the Campus Support Desk support call system. Core Services staff will then take appropriate action to ensure that the escalated item(s) is resolved.

- Team members are expected to close out all remediation work orders within the support call system and also alert the Core Services staff upon completion or escalation of each item.

Use of Information Technology

http://www.uc.edu/content/dam/uc/infosec/docs/policies/Use_of_Information_Technology_Policy.pdf

Contacts

Technology Services	513.732.5216

History