SYSTEM ACCESS AND USE MANAGING AND MONITORING PROCEDURE

Related Board of Trustees Policy: BP 8.4
Approval: August 2012
Revision:
NC Statewide Technology Standards: 20104 and 20109

Purpose: Procedure for managing network access controls.

Access to networks operated by Craven Community College is controlled to prevent unauthorized access and to prevent malicious attacks on the networks. Access to all College computing and information systems is restricted unless explicitly authorized.

- Remote users must connect to the Craven Community College network only using VPN protocols and software approved by the Technology Services department as outlined in the Remote Access Procedures.
- When users on the Craven Community College network connect to external systems, they shall comply with the Acceptable Use Policies and Internet Standards.
- Users should not install network hardware or software that provides network services, such as routers, switches, hubs and wireless access points, without written approval from Technology Services.
- Non-Craven computer systems that connect to the network will conform to all Craven Acceptable Use policies.
- Users should not download, install or run security programs or utilities that reveal weaknesses in the Craven Community College network without written approval from Technology Services. For example, Craven users must not run password-cracking programs, packet sniffers, network-mapping tools or port scanners while connected in any manner to the Craven network infrastructure. Users will not be permitted to alter network hardware in any way.

Monitoring System Access and Use

The College has the right and ability to monitor and filter use of information systems by employee and third-party contractor users.

- All use of Craven information resources is stored in server logs and accessible by authorized Technology Services staff only.
- All use of internet resources is filtered and monitored by an enterprise web monitoring system and accessible by Technology Services staff only.
- All datacenter access is recorded by camera systems and stored for later examination.
- Attempting to circumvent College monitoring controls, such as via the use of proxy avoidance servers, is not permitted.

Return to the Table of Contents