Remote Access Policy

1.0 Purpose

The purpose of this policy is to define standards for connecting to Kankakee Community College's network from any host. These standards are designed to minimize the potential exposure to Kankakee Community College (KCC) from damages which may result from unauthorized use of KCC resources. Damages include, but are not limited to, the loss of sensitive or college confidential data, intellectual property, damage to public image, damage to critical Kankakee Community College internal systems, etc.

2.0 Scope

This policy applies to all KCC staff, faculty and visiting faculty, students, alumni, guests, contractors, vendors and agents; hereto referred to as KCC authorized remote users, with a Kankakee Community College owned or personally-owned computer device used to connect to the KCC network. This policy applies to remote access connections used to access Kankakee Community College computing resources, including email, online courses, file access and any other computing resource that can be accessed remotely.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, FiOS, and cable modems, etc.

3.0 Policy

3.1 General

1. It is the responsibility of KCC authorized remote users with remote access privileges to Kankakee Community College's network to ensure that their remote access connection is given the same consideration as the user's on-site connection.
2. All KCC authorized remote users will be granted remote access privilege using ITS approved remote access methods as part of their normal network access. Some remote access methods will not be made available to all users by default.
3. No devices or software may be installed on KCC housed equipment, KCC owned or otherwise, that allows remote access to the KCC network. All remote access to KCC network resources is provided and provisioned by Information Technology Services.
4. General access to the Internet for recreational use by immediate household members through the Kankakee Community College network on personal computers is NOT permitted. The KCC authorized remote user bears responsibility for the consequences should the access be misused.

5. Please review the following policies when accessing the college network via remote access methods, and acceptable uses of Kankakee Community College's network:
    a. Acceptable Use Policy
    b. Network Connection Policy
    c. Virtual Private Network Policy

3.2 Requirements

1. Secure remote access must be strictly controlled. Control will be enforced via a one-time password authentication or public/private keys using strong passphrases. For information on creating a strong passphrase see the Computing Passwords Policy.
2. At no time should any KCC authorized remote user provide their login or password to anyone, including family members.
3. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
4. Non-standard hardware configurations, including security configurations, must be approved by Information Technology Services (ITS) before they can be implemented.
5. All hosts connecting to internal KCC systems not generally available to all Internet users will connect through a virtual private network (VPN) session to the college's centrally managed VPN server unless special dispensation is requested and granted.
6. KCC authorized remote users may be granted access to internal hosts without using a VPN session if there is an extenuating business reason and special dispensation is requested and granted by ITS. Only access from static IP addresses will be granted.
7. All hosts that are connected to Kankakee Community College's internal networks via remote access technologies must use the most up-to-date antivirus software, this includes personal computers.
8. Personal equipment that is used to connect to Kankakee Community College's networks must meet the requirements of KCC owned equipment for remote access.
9. Organizations or individuals who wish to implement non-standard Remote Access solutions to the Kankakee Community College network must obtain prior approval from Information Technology Services.

4.0 Enforcement

Any KCC authorized remote user found in violation of this policy will have their remote access privileges suspended immediately and without prior notice. Students, staff, and faculty found to have violated this policy may be subject to disciplinary action, up to and including termination of employment for staff and faculty.

5.0 Related Policies and Links

Acceptable Use Policy

Network Connection Policy

Virtual Private Network Policy

Questions or comments to: itpolicy@kcc.edu

Effective Date:

Last Revised Date: January 10, 2012