COMMUNITY COLLEGE OF DENVER

Title: VPN Access

Guideline #: IT – 1

Approved: June 3, 2011
July 13, 2015
August 9, 2017

References: Board Policy 3-125
State of Colorado Office of Information Technology

Approved By: Dr. Everette J. Freeman, President

---

1. PURPOSE

To create guidelines governing the usage of Virtual Private Network (VPN) access to the Community College of Denver (CCD or College) computer network to authorized staff.

2. APPLICABILITY

These guidelines apply for all remote access to the College's computer network and other resources.

3. DEFINITIONS

Virtual Private Network – A secure, encrypted, connection through the Internet to CCD network. A connected computer can access CCD resources as if it were physically located on campus.

4. POLICY

It is the College's policy that all employees comply with all computer and information systems guidelines as established by the College, Colorado Community College System (CCCS), and the State's Office of Information Technology.

5. GUIDELINES

The College's network contains private data and resources not available outside of our campuses. CCD's network also connects to the CCCS network, which contains similarly confidential information. Therefore CCD Information Technology Services (ITS) prevents access to this information from outside the CCD network. A secure VPN connection is available for users with a legitimate business need to access CCD resources remotely.

Eligibility – All full-time non-classified employees are eligible for VPN access and may apply by completing the VPN Access Request Form (IT-10) (Attachment A). All full-time classified employees must also use the VPN Access Request Form and obtain approval from the Director of Human Resources. Part-time employees are not eligible for VPN access. PERA retirees are eligible for VPN access and must follow the same guidelines as full-time non-classified employees. VPN access for contractors, consultants, and other parties will be considered on a case-by-case basis. Access and usage for all employees will undergo a yearly review by ITS.

IT Support of VPN – ITS will assist you in setting up VPN services on CCD-owned laptops. Although VPN usage on personal computers is permitted within the following guidelines, limited support will be provided for personal or non-CCD computers.

Requirements – All employees wishing to gain VPN access must fill out the VPN Access Request Form and agree to the following conditions and requirements:

a. Provide a business justification for their need to access CCD's network resources remotely.

b. Affirm that they will use VPN services in accordance with College and CCCS computing, security, and privacy policies.

c. Affirm that they will keep their computer up to date with all patches and other security updates for their computer's operating system.

d. Affirm that the computer(s) used to access the VPN run one of the approved anti-virus software packages listed below.

e. Affirm that they have a firewall installed on their home network or that they have a personal firewall installed on their computer.

f. Affirm that they will disconnect from the CCD VPN service when using their computer for personal use (such as web surfing or email).

g. Agree to perform only CCD business related activities while connected to the CCD VPN service.

h. Affirm that they will disconnect from the CCD VPN service when not using their computer or not accessing CCD administrative resources.

i. Affirm that they will save all work related files on CCD systems and remove such files from any personal computers before disconnecting.

j. Obtain appropriate signatures and approvals as designated on the VPN Access Request Form.

Permitted Anti-Viral Software – The following anti-virus packages have been reviewed and approved by ITS as acceptable packages to meet the anti-virus requirement. This list will be reviewed and updated periodically.

- McAfee Anti-Virus
- Bit-Defender Anti-Virus
- Trend Micro Anti-Virus
- Webroot Anti-Virus
- Norton Anti-Virus
- Kaspersky Anti-Virus
- AVG Anti-Virus (Full Edition Only)
- Vipre Anti-Virus

Policy Violations – Your signed VPN Access Request Form will be kept in your official CCD personnel file. Failure to comply with the CCD VPN policies may result in suspension of access or disciplinary action ranging from warning to termination. Sharing VPN access or information with other approved or non-approved individuals is strictly prohibited and will result in immediate and permanent suspension of VPN privileges. All CCD employees are required to report any unauthorized usage of CCD VPN or other network resources to ITS.