Columbia College: Remote Access Policy

Intent

The purpose of this policy is to define standards for connecting to Columbia College's network from any host. These standards are designed to minimize the potential exposure to Columbia College from damages which may result from unauthorized use of Columbia College's resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical Columbia College internal systems, etc.

Remote access implementations that are covered by this policy include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, and cable modems and other cloud file sharing tools. These devices could include, but are not limited to desktop computers, laptops, tablets and smart phones.

Guidelines

Telecommunications devices used to conduct Columbia College business must be used responsibly and ethically. Therefore, the following guidelines must be adhered to at all times:

- It is the responsibility of Columbia College employees, contractors, vendors and agents with remote access privileges to Columbia College's corporate network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Columbia College.
- It is also the responsibility of the user to ensure that the remote connection is logged out if he/she is not using the computer/device to access information. Leaving the connection open could permit malicious damage to Columbia College's electronic files and information.
- General access to the Internet for recreational use by immediate household members through the Columbia College Network on personal computers is not permitted. Laptop computers may have been provided by Columbia College for offsite work as it relates to the employee's position description and responsibilities. In these cases the laptop should only be used by the employee it has been assigned to, and for the purpose of completing their Columbia College duties.
- The Columbia College employee is responsible to ensure the family member does not violate any Columbia College policies, does not perform illegal activities, and does not use the access for outside business interests. The Columbia College employee will bear responsibility if the access is misused (through the progressive discipline process).
- All emails sent from the computer/device used for remote access must adhere to Columbia College's appropriate use guidelines and anti-harassment and bullying procedures.

Requirements

- Secure remote access must be strictly controlled. Control will be enforced via one-time password authentication or public/private keys with strong pass-phrases.
- At no time should any Columbia College employee provide their login or email password to anyone, not even family members.
- Employees are not permitted to save their passwords on the computer/device used for the remote access as another party could gain access to the computer/device.
- Columbia College employees and contractors with remote access privileges must ensure that their Columbia College -owned or personal computer or workstation, which is remotely connected to Columbia

College ’s corporate network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user.

- Columbia College employees and contractors with remote access privileges to Columbia College ’s corporate network must not use non- Columbia College email accounts (i.e., Hotmail, Yahoo, AOL), or other external resources to conduct Columbia College business, thereby ensuring that official business is never confused with personal business.
- Reconfiguration of a home user's equipment for the purpose of split-tunnelling or dual homing is not permitted at any time.
- Non-standard hardware configurations on Columbia College devices must be approved by Columbia College’s IT department, and the security configurations must be approved for access to hardware.
- All hosts that are connected to Columbia College internal networks via remote access technologies must use the most up-to-date anti-virus software; this includes personal computers.
- Personal equipment that is used to connect to Columbia College’s networks must meet the requirements of Columbia College -owned equipment for remote access.
- Organizations or individuals who wish to implement non-standard remote access solutions to the Columbia College production network must obtain prior approval from Columbia College’s IT department.

Acknowledgement and Agreement

I, _____(Employee Name), acknowledge that I have read and understand the Remote Access Policy of Columbia College. Further, I agree to adhere to this policy and will ensure that employees, if any, working under my direction adhere to this policy. I understand that if I violate the rules/procedures outlined in this policy, I may face disciplinary action, up to and including termination of employment.

Name: _____

Signature: _____

Date: _____

Witness: _____