Cochise College
Administrative Policy

Category: Technology
Policy Number: 6054
Title: Remote Access

The purpose of this policy is to define how Cochise College controls remote access to college information systems and networks in order to minimize the potential exposure to damages that may result from unauthorized use. Damages include the breach of sensitive or confidential information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system availability, or the corruption of information integrity.

Procedure: 6054.1
Scope

This policy applies all college employees, contractors, consultants, temporaries, agents, workers, affiliates, and other third parties utilizing Virtual Private Network (VPN) or remote access connections to access the college's network. All such connections must be via the approved VPN client or other approved method.

Procedure: 6054.2
Roles & Responsibilities

Information Security Team: The Information Security Team is responsible to ensure compliance with this policy as a component of the College's information security program.

Remote Access Users: All remote users agree to comply with this policy and apply safeguards to protect Cochise College information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include protection of their remote access credentials and the use of discretion in choosing when and where to use remote access to data or services in an effort to prevent inadvertent or intentional viewing of displayed information.

Procedure: 6054.3
Policy

Employees and third parties authorized to utilize remote desktop or VPN connections shall ensure that unauthorized users are not allowed access to the Cochise College internal network. All individuals and machines, while accessing the network, including College-owned and personal equipment, are a de facto extension of Cochise College's network and therefore these systems are subject to the same rules and regulations stated in the college's information security policies. Users of computers that are not college property shall configure the equipment to comply with the *Computer and Server Security Standards*.

Remote desktop and VPN connections shall:

- Use a public/private key encryption system supporting at least 256-bits for remote desktop and at least 1024-bits for VPN
- Use two factor authentication for remote access
- Require strong passwords for authentication. For information on creating a strong pass-phrase see the *Passphrase Complexity and Protection Policy*.
- Be automatically disconnected from college's network after fifteen minutes of inactivity
- Not be connected to any other external network at the same time.

No devices or software may be installed that allows remote access to the network such as modems, wireless access points, or VPN servers. All remote access will be provided centrally by IT.

Any remote access using either remote desktop, VPN, or any other remote access to the organizational network must be reviewed and approved by the appropriate supervisor. All employees by default will have account settings set to deny remote access. Only upon approval will the account settings be changed to allow remote access.

All hosts that are connected to the network via remote access technologies must use the most up-to-date anti-virus software, and be up-to-date on available patches. This includes personal computers. Security patches for installed operating systems (ideally with auto-update enabled), web browsers, and common applications shall be applied in a timely manner. A personal firewall must be installed and enabled on each host.

Remote access services may be used only for the conduct of college related business. Personal, family, private or other commercial use of any service available remotely is not permitted.

Remote access services may not be used to transfer or copy sensitive, restricted or internal data as defined by the *Data Classification Policy* residing on college file shares or other College-owned information systems to external systems, including privately owned computers or mobile devices.

Procedure: 6054.4
Periodic Review

All accounts provided for remote access to Cochise College resources must be reviewed on at least an annual basis to ensure access is restricted only to authorized individuals.

Cochise College retains the right to amend the terms of the remote access policy at any time, and to alter, change, suspend or terminate remote access service as may be required at any time in its sole discretion.

Procedure: 6054.5
Compliance

This policy is a component of Cochise College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA and other regulations.

Procedure: 6054.6
Exceptions

The Chief Technology Officer (CTO) or a designated appointee is authorized to make exceptions to this policy.

Procedure: 6054.7
Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Cochise College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

Procedure: 6054.8
Definitions

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Remote Access: Remote Access is term used to describe connectivity to the network from devices not directly connected to the network, such as those located in a private residence or other offsite location. All remote access to systems, with the exception of accessing email via a web browser or handheld device, is to occur via encrypted remote desktop or VPN connections.

User: Any Cochise College faculty, staff, students or partner who has been authorized to access any college electronic information resource.