Washtenaw Community College

Remote Access Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

Remote Access refers to the ability to connect to the College network from off-campus and make use of resources on it as if on campus. The College makes use of Virtual Private Network (VPN) technologies to establish a secure encrypted session or tunnel over public networks between a client system and the College network.

The purpose of this policy is to define how Washtenaw Community 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 or intellectual property, damage to critical internal systems, compromise of system availability, corruption of information integrity, or damage to public image.

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.

ROLES & RESPONSIBILITIES

Information Security Office: The Information Security Office 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 Washtenaw Community 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.

REQUIREMENTS & PRACTICES

Employees and third parties authorized to utilize remote VPN connections shall ensure that unauthorized users are not allowed access to the Washtenaw Community College internal network. All individuals and machines, while accessing the network, including College-owned and personal equipment, are a de facto extension of Washtenaw Community College's network and therefore are subject to the same rules and regulations stated in the College’s information security policies.

If you are unsure as to your ability to comply with the following requirements, please be advised that remote access to protected institutional resources can put the college at significant risk and you should not proceed with remote access using such devices.

Users of Remote VPN connections shall adhere to the following requirements:

- Only college-owned devices or personal computers in compliance with this policy are to be used for remote access
- All client systems that are connected to the College network via remote access technologies are expected to have taken precautions to avoid common security vulnerabilities, including:
    - Use of up-to-date anti-virus software
    - Ensure that client systems and applications are up-to-date on available patches, including 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 should be installed and enabled on each client system
    - Ensure that a screen lock is used whenever the remote session is unattended

- Users of computers that are not College property shall configure the equipment to comply with the *Server and Computer Configuration Standards*
- 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 College 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. For example, sensitive data residing in a folder on the departmental shared drive should be accessed remotely as opposed to being transferred or copied to the remote system.
- All remote connections must be via the approved VPN client. No other VPN, Remote or Virtual Desktop connectivity or remote access application (e.g. SSH, LogMeIn, VNC) is approved, supported, or permitted.
- No connections to secondary networks are permitted while using a remote VPN session to the College network, i.e. no split tunneling, dual homing, or rerouting of portions of client traffic to bypass the established VPN session.
- No devices or applications may be installed on systems connected to College networks that enable remote access to the network, e.g. modems, wireless access points, or VPN servers. All remote access is centrally provided by Information Technology Services (ITS).

IT administrators of Remote VPN connections shall:

- Use a public/private key encryption system supporting at least 256-bits
- Use multi-factor authentication for remote access
- Require strong passwords for authentication. For information on creating a strong password see the *Password Complexity & Management Policy*.
- Ensure remote sessions are automatically disconnected from College's network after fifteen (15) minutes of inactivity

- Enforce the requirement, where possible, that all endpoint traffic be directed and encrypted via the VPN tunnel established with the College network, i.e. no split tunneling, dual homing, or rerouting of traffic beyond intended endpoint.
- Requests for remote access must be reviewed and approved by the appropriate supervisor, Human Resources, and ITS. 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.

COMPLIANCE

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

EXCEPTIONS

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

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

DEFINITIONS

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

Dual Homing: Having concurrent connectivity to more than one network from a computer or network device.

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.

Split Tunneling: A computer networking concept which allows a mobile user to access dissimilar security domains like a public network (e.g., the Internet) and a local LAN, WAN, or Private VPN at the same time.

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

REFERENCES

Data Classification Policy

Password Complexity & Management Policy

Request for Policy Exception

Server and Computer Configuration Standards

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO