This procedure is meant to enhance the Western Michigan University (WMU) policies and procedures related to remote access of information technology. It is not exhaustive. It does not contain all policies and procedures of WMU. WMU policies and procedures can be found on individual central office websites or by contacting the responsible department. Refer to the Remote Access Policy on the Office of Information Technology’s website for additional information. This procedure is meant to protect confidentiality and University data.

**SCOPE**

- If an employee has a work-related need to work from home, away at a conference, or at another remote location and needs to access the University network from any device (whether personally owned or University owned), the employee must first obtain approval from her/his immediate supervisor and provide the approval to the Director of Information Technology using this form. Approval is necessary for employees who need to remotely access University data classified as confidential. It does not include email, GoWMU, D2L, and/or any University publicly accessible websites.

**REQUIREMENTS**

Device Type __________________________________________________________________________

Employee initials  __________________________________________________________________________

_____ I understand and agree to adhere to the WMU Remote Access Policy.

_____ I agree that the device used for remote access contains antivirus software with updates enabled.

_____ I agree that the device used for remote access has security patches for installed operating systems, web browsers, and common applications are applied in a timely manner.

_____ I agree to use the VPN for confidential information and will not save the confidential information on a device hard drive or other local resource.

_____ I agree to submit the necessary device information to the Director of Information Technology.

_____ I understand and agree to semiannual security audits to assure that no unnecessary, confidential/protected data is being stored on the device.

________________________________________________________________________________________
Employee Printed Name  ____________________________  Employee Signature & Date

________________________________________________________________________________________
Supervisor Printed Name  ____________________________  Supervisor Signature & Date

________________________________________________________________________________________
Director of Information Technology