Technology Checklist for UM Telework and Remote Work

This checklist can be used to ensure that the employee has the appropriate security and applications to continue their work while teleworking or working remotely. If you require assistance in completing this form, downloading applications, etc., please contact the UM IT Helpdesk.

Category	Description	Verified
Home internet connectivity	The employee is responsible for maintaining a broadband connection adequate to job function.	
Home network security	Wireless networks used for telework must be encrypted using a WPA2 key. Default passwords for networks and routers must be changed by the employee to strong, unique values. Instructions and support for these settings are available from the employees Internet Service Provider of the router manufacturer.	
VPN	UM provides a secure Virtual Private Network (VPN) connection via the Cisco AnyConnect VPN client. Remote workers will have to install this client and connect to the UM VPN before accessing any sensitive UM data systems from off campus.	
University computers	Sensitive UM data should only be handled on UM-owned computers.	
Communication Platform	Employees may be required to be virtually present via a UM or department-approved online collaboration tool (Zoom, Teams, etc.) during agreed-upon working hours.	
Applications	The UM IT Helpdesk can help ensure all applications needed for remote work are installed and properly licensed.	
Data	UM data used by teleworkers is subject to all of the security and backup provisions of the UM IT Security and Confidentiality Policy. One convenient way for employees to meet these requirements is to store UM data on approved UM data storage services as defined in that policy.	
Printing	Personally-owned and home printers must not be used to print sensitive university data. Your own home printer cannot be supported by UM IT. If necessary, print remotely back to campus using secure print settings to ensure data security.	
University telephone system	Teleworking employees should be reachable at UM-assigned telephone number during working hours. UM Telecommunications offers several options for employees to configure their phone lines to enable off-campus communications.	

Support	The UM IT Helpdesk and related organizations will not send employees to teleworkers' homes to provide service under any circumstances. Teleworking employees accept responsibility for the maintenance of certain systems crucial to their work, including but not limited to home networks and internet connectivity. Support for these services should be carried out by the individual employee or by a third-party contractor (eg, an ISP) paid by the employee. University-owned equipment can be serviced by the UM IT Helpdesk. Much service can take place remotely; however, teleworking employees should understand that some computer service will require the employee to bring the device in to the UM IT Helpdesk.	
Contingency Planning	Supervisors and employees should discuss and document contingency plans for common failure modes of remote work, including but not limited to failures in home networking or internet connectivity.	

Supervisor Name: _____ _____

Print Name Signature

Employee Name: _____ _____

Print Name Signature

_____

UM Employee Number

Date Checklist Completed: _____