Remote Access Standard

June 2026

Purpose:

This standard outlines requirements for remote access to university information resources and is designed to protect these resources from unauthorized access or use and reduce the risk of security incidents.

Definitions:

Highly Confidential Data: University Data which, because of its associated legal restrictions or potential security ramifications, is approved for use only on a very limited basis and only with special security precautions. See Highly Confidential Data list.

IT-VPN: JMU's centrally managed VPN installation that allows an individual from outside of the JMU network to access internal JMU network resources through a secure encrypted network connection over the Internet following the successful authentication of the individual.

Netskope Private Access (NPA): allows 'always on' connectivity for JMU owned and managed Microsoft Windows and Apple macOS computers to access internal network resources.

Protected Data: University Data individually requested and approved by a Data Manager for a specific business use and subject to the general provisions associated with university information security. This includes, but is not limited to, Personally Identifiable Information (other than PII classified as highly confidential) worthy of protection and discretion in its distribution and use.

Remote Access: Access to JMU's internal network from a non-campus network through Information Technology centrally managed devices as well as self-administered or personally owned devices. Examples include IT-VPN and NPA.

University Data: Data collected, maintained or used by university personnel, contractors, or partners as part of their job responsibilities, for operation of the University, or to fulfill its mission. University Data may reside in different automated systems and in different physical locations, but are to be considered part of a single, shared resource. This resource consists of information represented in a variety of data elements, types, and forms maintained by individuals, administrative/ academic units or business partners to provide functionality to the University. All such data owned and managed by or on behalf of the University are considered University Data unless explicitly noted otherwise in writing.

Virtual Private Network (VPN): A virtual network built on top of existing networks that can provide a secure communications mechanism for data and IP information transmitted between networks. These virtual networks may be host to network, or site to site.

Standard:

1. Remote Access:

All authorized JMU students, employees, and affiliates may utilize the benefits of remote access to university information resources for which they have been granted access. Employees who

access University Data classified as highly confidential or protected are required to use a university-owned and managed device. The use of remote access services, other than IT-VPN and NPA, must receive approval from the Information Security Officer or designee. Encryption technology used must follow best practices and be an industry standard algorithm.

Unattended remote administration tools which provide direct access to campus endpoints (e.g., TeamViewer, LogMeIn, GotoMyPC) are prohibited. Exceptions may be granted for vendor remote support purposes on a case-by-case basis by submitting a ticket to IT Security.

Remote access may not be permitted from some locations, such as embargoed or sanctioned countries.

JMU Information Technology reserves the right to monitor for unauthorized remote access and disable access of those devices providing a non-sanctioned service.

2. IT-VPN:

JMU students and employees receive access to library resources by default. IT-VPN access to specific resources may be provided by submitting a Remote Access Request to Information Technology. For employees, the user requesting to obtain remote access and their supervisor must approve the Remote Access Request prior to access being granted. Affiliates may be provided specific access through a Remote Access Request approved by the affiliate sponsor. All required approvals must be satisfied before access is granted.

IT-VPN user access is controlled via JMU centrally managed multifactor authentication.

IT-VPN connection time is limited to an absolute continuous connection time of 12 hours. Users may reconnect if necessary. Inactive IT-VPN sessions time-out is limited to no more than 4 hours.

3. NPA:

This service is provided to JMU owned and managed Microsoft Windows and Apple macOS computers and does not require end user approval.