[Nu-vpn-users] VPN Security Posture Beginning July 5

Phil Redfern <phil.redfern@nebraska.edu>

Tue 2023-06-06 08:28

To:nu-vpn-users@lists.nebraska.edu <nu-vpn-users@lists.nebraska.edu>

Beginning July 5, the following security posture elements will be required for university employees when accessing network-restricted Medium Risk Information Systems from the VPN. Network-restricted Medium Risk Information Systems may include internal research, administrative, or other business systems. University-owned and managed computers are configured to meet these security posture requirements according to their risk classification. The following security resources are available for university employees that leverage personally-owned devices to conduct university business.

Instructions for Configuring Security Elements on a Personal Device

- Supported Operating System with Automatic Updates Enabled
- Full Disk Encryption
- OS Firewall Enabled
- Cortex XDR

The following are examples of common university services that are not network-restricted and will continue to be accessible from any device without a VPN.

- Firefly Employee Self Service
- MyBlue, MyRed, MyNCTA, & MavLink
- Learning Management System (Canvas)
- eSignature System
- Office 365 (University email, Teams, OneDrive, SharePoint, etc.)
- Multi-factor Authentication (Duo)
- Zoom

If you have any questions about these requirements for accessing University of Nebraska Information Systems with the VPN, please contact your IT Support Team for assistance.

Phil Redfern
Director, Security Engineering
Office: 402-472-7959
phil.redfern@nebraska.edu
https://its.nebraska.edu
UNIVERSITY OF Nebraska System