VPN Request (Vendor)

Customer Procedure

Primary Point of Contact: Chad Hrivnyak

Overview:

IT Security processes firewall Vendor VPN requests when properly sponsored and justified.

Customer Procedure:

Authorization for VPN access for vendors or external organizations will be processed through the IT help desk, 419-530-2400. Vendor access must have a sponsoring university manager’s approval and justification.

The following information is required to request Vendor VPN access:

1. Do we have existing services established with this vendor? If so, we may need to just modify our current setup. If not, then this would be a request for new service.

2. Do we have legal paperwork with this vendor (i.e. business associate agreements, contracts, service-level agreements, etc.)? If not, these must exist prior to enabling remote access to the UT network. They must specifically state how the vendor will conduct business with UT and how they handle UT data. There may be multiple compliance requirements that must be met in addition. **Do NOT proceed with requesting access if this has not been determined and established.**

3. What are the vendor’s technical capabilities? We must know if they can support direct VPN connections, otherwise VPN client software or other alternatives may be necessary.

4. How does the vendor handle support for other customers? We try to support their standards, but sometimes there are conflicts with our internal processes. We also try to avoid making the process too complicated for their staff, but there may need to be a compromise on how this is implemented.

5. Provide exact details of:
   a. Technical contact details for network team or support staff, including names, titles, email addresses, telephone numbers, web addresses or any other useful communication information.
   b. Timeline of implementation/project. This will better coordinate the enabling, testing, and troubleshooting prior to launch.
c. Host names / IP Addresses / Subnet Masks of all systems involved

d. Ports / Protocols used. No protocol will be inherently enabled by default, so all must be included.

e. Applications supported

f. Hours of access required

g. Frequency of access expected

6. IT Help Desk submits the VPN/Firewall Request.

Measure of Completion:

VPN access requests for vendors are considered closed when the associated Remedy Ticket is closed.