**VPN ACCESS FORM**

**Virtual Private Network (VPN) Policy**

**Purpose**

Virtual Private Network (VPN) service at Tarlac State University is managed and provided by Tarlac State University – Management Information Systems Office (MISO) for members of the University who require remote and secure access to Tarlac State University’s MISO file servers, print servers, software licensing and various web-based services when at home or traveling. In an effort to ensure the security and integrity of the service, certain requirements and guidelines must be met by the administrators and users of this service. The Virtual Private Network (VPN) service provided by MISO strongly recommends TSU network users to use the VPN connection when connecting to Tarlac State University resources over any unsecured (open or public) wireless network.

**Intended Use**

VPN access is provided for the TSU community by MISO provided that users adhere to all established policies relating to the use of the Tarlac State University network and associated technology resources as well as applicable local and national laws. Remote computers attaching to the VPN become an extension of the Tarlac State University data network and are therefore subject to the same network use guidelines and policies extended to any other host on the network.

**Usage Policy**

1. TSU employees may utilize the benefits of VPNs, which are “user managed” service. This means that the user is responsible for selecting an Internet Service Provider (ISP) and coordinating required software installation.
2. It is the responsibility of TSU employee with VPN privileges to ensure that unauthorized users are not allowed access to internal networks of TSU.
3. VPN use is to be controlled by the user’s Active Directory credentials, as managed by the user on University-issued workstation.
4. VPN users will be automatically disconnected from the TSU network after a predetermined amount of inactivity. The user can immediately log on again to reconnect to the TSU network. Likewise, all authentication attempts will be logged.
5. It is the responsibility of all VPN users to seek approval from the process owner of the system and approval from the Office Head and respective Vice Presidents. Only those with prior approval will be accommodated.
6. Users and machines connected to the VPN must abide by all policies of MISO including, but not limited to, the TSU IT Policy, Non-Disclosure Agreement and Data Privacy Law.
7. If any violation of policy occurs, Tarlac State University may take any necessary step in ensuring the security of the VPN and the greater network. This may include temporary suspension of accounts and/or network access.
8. MAC address of the device will be collected for monitoring purposes.
9. VPN connectivity will be set up and managed by the MISO based on the allowable (limited) simultaneous users of the VPN device.
10. Technical evaluation or assessment may be required prior to request for exemption. Any exception to the policy must be approved by concerned authorities.

|  |
| --- |
| **Consent statement:**Tarlac State University will collect your personal information only for the purpose indicated in the form. All information will be kept confidential and secured in compliance with the Data Privacy Law. |
| **Declaration:** I commit to adhere to the university’s VPN Policy for access to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_from \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.**Systems / Applications to be accessed:**⬜ PRINCE / PRISMS / Enrollment System⬜ PMAPS / HRIS ⬜ Time Attendance⬜ Payroll Support⬜ Automated Faculty Evaluation System / AFES⬜ Business Center Inventory System⬜Data Bank Management System⬜ENGAS⬜ Others, please specify: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Requested by:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Name and Signature of Requestor**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Name and Signature of Immediate Supervisor**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date Requested | Recommending Approval:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**Director / Dean** |
| **Approved:**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **VPAA / VPA / VPRDE / OUP** |
| **For MISO use**Device MAC Address: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date Received: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Processed by: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |