Virtual Private Network (VPN) Policy
COE–VPN–01

1.0 Purpose
The purpose of this policy is to provide guidelines for Remote Access IPSec Virtual Private Network (VPN) connections to the College of Engineering University network.

2.0 Scope
This policy applies to all College of Engineering employees, contractors, consultants, temporary personnel, and other workers including all personnel affiliated with third parties utilizing VPNs to access the College of Engineering network. This policy applies to implementations of VPNs that are directed through an IPSec Concentrator.

3.0 Policy
VPNs provide a method of encrypting data traffic when using an external Internet Service Provider (ISP) or wireless access points. College of Engineering employees and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs. Further details may be found in the Remote Access Policy and Wireless Communication Policy.

Additionally,
1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to the College of Engineering internal networks.
2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase. Further details may be found in the Password Policy.
3. VPN gateways will be set up and managed by the College of Engineering network operational group.
4. All computers connected to the College of Engineering internal networks via VPN or any other technology must use the most up-to-date anti-virus software available.
5. Users of computers that are not College of Engineering-owned equipment must configure the equipment to comply with the College of Engineering's VPN and Network policies.
6. Only College-approved VPN clients may be used.
7. By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of the College of Engineering's network, and as such are subject to the same rules and regulations that apply to the College of Engineering-owned equipment, i.e., their machines must be configured to comply with College Security Policies.

4.0 Enforcement
Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

5.0 Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPSec Concentrator</td>
<td>A device in which VPN connections are terminated.</td>
</tr>
</tbody>
</table>

6.0 Revision History

Last updated: 11/25/2003