



<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>1 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

**1.0 PURPOSE**

The purpose of this document is to provide the framework for granting remote access to Collin County services/equipment through a Virtual Private Network (VPN).

**2.0 SCOPE**

This policy applies to Collin County employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPN to access the Collin County network. This policy applies to all Collin County VPN implementations.

**3.0 POLICY**

Authorized parties (Collin County employees, customers, vendors, government agencies, etc.) may utilize the benefits of VPN, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees.

**Additionally,**

1. It is the responsibility of the user with VPN privileges to ensure that unauthorized users are not allowed access to Collin County internal networks. User accounts and passwords are NOT to be shared with anyone.
2. Authorized parties and the Collin County employees sponsoring the request for VPN are responsible for defining what services/equipment the authorized parties need access to. Access will be restricted to only those defined objects. Attempting to connect or access any service/device not defined will be considered a violation of the Collin County VPN policy.
3. The authorized parties and the Collin County employees sponsoring the VPN request are also responsible for defining the time scope that the VPN account will be active. All accounts are setup with an expiration date not to exceed 6 months.
4. 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 pass phrase.
5. When actively connected to the county network, the VPN will force all traffic to and from the remote PC over the VPN tunnel; all other traffic will be dropped.
6. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
7. VPN gateways will be established and managed by Collin County Infrastructure

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------



<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>2 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

Department.

8. All computers connected to Collin County internal networks via VPN or any other technology must use the most up-to-date anti-virus software from a reputable IT vendor; this includes personal computers. The anti-virus software must be updated with the latest definition files from that vendor.
9. All users connecting to the Collin County internal networks via VPN or any other technology must keep their systems up to date with the latest security patches for their operating system and applications installed on their connecting systems.
10. VPN users may be automatically disconnected from Collin County’s network after sixty minutes of inactivity. The user must then logon again to reconnect to the network.
11. Users of computers that are not Collin County owned equipment must comply with the Collin County acceptable use policy when accessing the Internet while connected through the VPN.
12. Only approved VPN clients may be used.
13. Upon termination of a contract from Collin County, or at the request of the Collin County staff, the user must uninstall the VPN connection from their computer.
14. Vendors expressly agree to notify the County of staffing changes involving employees or subcontractors with access to the County’s network within 24 hours or next business day.
15. Customer and vendor accounts will only operate in a defined date range. They will only be operable during project implementation or on an as needed basis for remote support. Remote support will only be activated by calling Collin County and requesting access to the VPN. This request must include an end date when remote support will no longer be needed. After those events have been completed the VPN accounts will be disabled.
16. After six months of expired inactivity, Active Directory and VPN accounts will be permanently deleted.
17. Accounts may be locked out after a certain number of failed attempts.
18. VPN users who have lost their password will have to contact their sponsoring parties to request a password reset. The sponsoring party will then contact Collin County IT to reset the password for the VPN user.
19. It is the responsibility of the user with VPN privileges to install, configure and setup their systems to connect to Collin County based on the information provided to them.
20. Users connect at their own risk and Collin County is not responsible for any damages that they may incur from connecting through the VPN to Collin County
21. Prior to acquiring VPN access all users will be required to pass a background check.

### Granting Access

1. To obtain access via VPN, the vendor/Agency/User must be sponsored by a party currently employed at Collin County and IT must agree this access is needed for the Collin County information systems. The vendor/agency/user must sign the “Connection Policy and Agreement Form” form agreeing to protect the security of the Collin County network. For external Collin County VPN users, the Request for VPN Access must be signed and approved by the Manager who is responsible for the external user. VPN expiration will be based on the contract length unless further time is requested by Collin County Management.

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------



<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>3 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

**Enforcement**

1. Collin County Infrastructure Department may actively monitor the VPN concentrator for any suspicious and inappropriate activity. Any VPN user found to have violated any part of this policy may have their VPN access terminated immediately.

**Liability**

1. Vendor expressly agrees that they shall be liable for any and all damages, including but not limited to actual, consequential, or incidental damages, for disruptions caused by their negligence or intentional misconduct to the County’s services/equipment resulting from or related to Vendor’s connection to the County’s networks. Vendor also expressly agrees to notify the County of staffing changes involving employees with access to the County’s network within 24 hours or next business day.
2. Unauthorized access or use is prohibited and will be prosecuted to the fullest extent. Anyone using this system expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personnel may provide the evidence of such monitoring to law enforcement officials. Anyone using the system connects at their own risk and assumes all responsibilities for any possible damage to their own equipment.

**4.0 PROCEDURES**

**To obtain access to VPN for a project or for to support Collin County the following steps will be followed**

1. The vendor must prove that they don’t have an alternate way of connecting to Collin County to provide the services they are requesting access for. This includes the use of products like WebEx that proved support on an as needed basis and are initiated by a user within Collin County. This does not include products such as GotoMyPC or LogMeIn; products that open connections from the inside on an always on basis and do not require Collin County user participation. Those products are prohibited from being used.
2. The vendor/Agency/User must be sponsored by a party currently employed at Collin County (this may be someone in IT) and IT must agree this access is needed for the Collin County information systems. The vendor/agency/user must sign the “Connection Policy and Agreement Form” form agreeing to protect the security of the Collin County network. For external Collin County VPN users, the Request for VPN Access must be signed and approved by the Manager who is responsible for the external user. VPN expiration will be based on the contract length unless further time is requested by Collin County Management.
3. The vendor/agency/manager/user/sponsor must sign the “Connection Policy and Agreement Form” form agreeing to protect the security of the Collin County network. For external Collin County VPN users, the Request for VPN Access must be signed and approved by the Manager who is responsible for the external user and the sponsoring party.
4. A background will be run on the user requesting VPN access.

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------



<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>4 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

5. The vendor/agency/user and sponsoring party will identify what services/equipment will be accessed through the VPN tunnel. They will also identify the time scope that this account will be enabled for that is not to exceed 6months.
6. The sponsor will create a Track-IT ticket (with or without the help of IT) for this services request.
7. After the above is complete the VPN user information and services/equipment to be accessed will added to the new Track-IT ticket for this request.
8. The active directory account will be created...
  - a. With appropriate rights to access the systems/equipment
  - b. With an expiration date not to exceed 6months
  - c. Password will be generated based on the following
    - i. At least
      1. 8 characters
      2. 1 upper case letter
      3. 1 lower case letter
      4. 1 special character (e.g, &, #, \$, \*, etc.)
    - ii. Not do any of the below
      1. Be the default password for any system
      2. Be any word from any language
      3. Use adjacent keys on the keyboard like “qwerty”
      4. Use consecutive sequence of letters or numbers like “abc” or “123”
9. The person setting up the VPN connection will
  - a. Create an account on the Cisco ACS server matching the username of the AD account
    - i. This account will use Windows NT/2000 (active directory) for password authentication
    - ii. The “Real Name”, “Description”, “Vendor/Department” and “Creation Date/Initials” will be filled in
    - iii. The appropriate group will be chosen for the connection
    - iv. All other fields will be left at their default values
  - b. On both VPN ASA’s the VPN will be setup
  - c. For outside customers, vendors and government agencies the following will be setup
    - i. New group policies to apply security settings to. The name of which will be descriptive for easier administrative capabilities
    - ii. New IP address range for connecting computers
    - iii. Pre-shared key for Cisco VPN connection
    - iv. Object groups that identify by IP address what services/equipment user will be connecting to
    - v. Access list defining what VPN users has access to based on the object groups
  - d. Test VPN connection to verify that the requested services/equipment are accessible and other not requested services/equipment is not accessible
  - e. Contact by phone (not in e-mail, IM, or text messaging) the sponsor and provide the login credentials/information for the VPN
  - f. If needed the VPN client will also be provided

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------

<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>5 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

10. The sponsor will contact the VPN user by phone (not in e-mail, IM or text messaging) and give them their login information

**For getting access after the VPN has been granted but the account is in the expired or disabled state**

1. The user of the VPN will contact their sponsor and request access to the VPN stating the following
  - a. Reason for this access
    - i. To provide support for Collin County
    - ii. To extend the amount of time to complete a project
    - iii. To recertify that the VPN account is still needed and in use
  - b. The duration of the access needed not to exceed 6months
2. The sponsor will open a Track-IT ticket (with or without the help of IT) and place this information in the ticket.
3. Helpdesk will then process the Track-IT ticket and contact the sponsor when the request has been completed.
4. The sponsor or IT will contact the VPN user to update them on the Track-IT request

**For password resets**

1. The VPN user will contact their sponsor and request that their VPN password be reset
2. The sponsor is responsible for validating the identity of the user and that it does match the VPN account they are requesting the password reset on.
3. The sponsor will open a Track-IT ticket (with or without the help of IT) and request the password reset
4. Helpdesk will then process the Track-IT ticket and contact the sponsor when the request has been completed.
5. The sponsor will contact the VPN user by phone (not in e-mail, IM or text messaging) and give them their login information.

**For decommissioning of VPN accounts**

1. When contact is made from the vendor/user/sponsor/IT that an account needs to be decommissioned a Track-IT ticket will be generated and Helpdesk will disable the active directory account. This will put the VPN account out of service.
2. Periodic audits will be run and all accounts that have been expired or disabled for over 6months may be deleted from both active directory and Cisco ACS servers. The VPN ASA's configuration information will also be removed from both VPN ASA's.

**Connection banner displayed every time someone connects through VPN**

Unauthorized access or use is prohibited and will be prosecuted to the fullest extent. Per the Collin County VPN policy you must have the most up-to-date anti-virus software from a reputable IT vendor installed on your connecting computer. The anti-virus software must be

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------

<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>6 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

updated with the latest definition files from that vendor. Your connecting computer must also be up to date with the latest security patches for your operating system and applications installed on your connecting system. To use this VPN system you must have agreed to and signed the Collin County “Connection Policy and Agreement Form”, and been personally granted access by Collin County IT. If you do not meet the above requirements disconnect now and address the issues before connecting again. Using this VPN system means you are expressly consenting to the monitoring of your activity on the Collin County network. Anyone using this VPN system connects at their own risk and assumes all responsibilities for any possible damage to their own equipment.

## 7.0 REVISION HISTORY

This is an update to the original Collin County VPN Policy.

Date	Revision #	Description of Change
01/01/2010	1.0	Initial creation – Draft
03/26/2010	2.0	New VPN Policy

## 8.0 INQUIRIES

This section tells the reader where to go for additional information on this policy.

## 9.0 APPENDICES

Term	Definition
VPN.	Virtual Private Network. An extension of Collin County’s internal private network.
VPN Concentrator.	Physical device that manages VPN connections.
VPN Client.	Remote computer with VPN software utilizing VPN services.
Dual (split) tunneling.	When utilizing VPN, a connection (tunnel) is created to Collin County’s network utilizing the Internet. Dual split tunneling allows for this connection as well as a secondary connection to another source. This technology is NOT supported when utilizing Collin County’s VPN.
User	Contractor, consultant, temporaries, customers, etc.
Vendor Management	Person in vendor company that can take

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------

<b>Policy #:</b>	<b>ITP-N018-VPN Policy</b>	<b>Effective:</b>	<b>07/01/2010</b>	<b>Page #:</b>	<b>7 of 7</b>
<b>Subject:</b>	<b>Title: New – N018 – VPN Policy</b>				

	responsibility for the liability clause of this document.
Sponsoring Party	Collin County employee requesting access for a non-employee user to have access to Collin County services/equipment through the VPN. The employee may be someone in IT.

<b>Revision #:</b>	2.0	<b>Supersedes:</b>	1.1	<b>Date:</b>	04/01/2010
--------------------	-----	--------------------	-----	--------------	------------