ATTACHMENT A

Connection Policy and Agreement Form

Virtual Private Network (VPN)

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, government agencies, 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, unless otherwise authorized to be a longer timeframe or permanent by the County.
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 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, on an as needed basis, or per the County contractually agreement 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, unless otherwise approved by the County.

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 unless otherwise approved by the County.
22. If the County migrates to a new network connection technology it is the responsibility of the vendor or agency to budget and obtain any required technology upgrade in order to maintain their network connection to the County. The vendor or agency will be provided advance notification for this change.

4.0 Granting Access

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 this 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. The initial setup and testing will be perform during normal operating hours, Monday – Friday, 8 am – 5 pm, and requires a minimal or two weeks' notice to schedule.

5.0 Enforcement

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.

6.0 Liability

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.

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.

7.0 Definitions

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.
Vendor Management	Person in vendor company that can take responsibility for the liability clause of this document.
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	Employee, vendor, contractor, consultant, temporaries, customers, government agencies, etc.
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.

ATTACHMENT A

Vendor Management's Signature (if applicable)

Printed Name: _____ Signature: _____

E-Mail Address: _____ Phone: _____ Date: _____

VPN Users Signature

Printed Name: _____ Signature: _____

E-Mail Address: _____ Phone: _____ Date: _____

Sponsoring Party's Signature

Printed Name: _____ Signature: _____

E-Mail Address: _____ Phone: _____ Date: _____

Return form to:

Caren Skipworth
2300 Bloomdale #3198
McKinney, Texas 75071