COLLIN COUNTY

Information Technology
2300 Bloomdale Road
Suite 3198
McKinney, Texas 75071
www.collincountytx.gov

| Policy #: | 033 | Effective: | 01/01/2013 | Page #: | 1 of 7 |
|---|---|---|---|---|---|
| Subject: | Title: External Entity VPN Tunnel Policy | | | | |

## 1.0 PURPOSE

The purpose of this document is to provide the framework for creating remote access to specific Collin County services and/or equipment through a Virtual Private Network (VPN) tunnel from specific equipment within an external agency.

## 2.0 SCOPE

This policy applies to agencies external to Collin County (i.e. government entities, agencies, contractors, consultants, etc.) utilizing a VPN tunnel from their network to access the Collin County network. This policy applies to all Collin County VPN tunnel implementations.

## 3.0 REFERENCE

Refer to Collin County policy number 018 – VPN Policy which documents a correlated policy for VPN access granted to Collin County personnel.

## 4.0 BACKGROUND

This policy document was created in response to an influx of requests from governmental entities requesting connection to Collin County.

## 5.0 POLICY

To facilitate inter-agency cooperation and data sharing, authorized external agencies (i.e. government entities, law enforcement agencies, contractors, consultants, etc.) may utilize the VPN tunnel as a "user managed" service. As a “user managed” service, the agency is responsible to provision, configure, maintain and support appropriate Cisco VPN equipment (per Collin County technology standards), procure appropriate communication channel(s), troubleshoot VPN tunnel communication issues and train their staff on the connection method(s) required to utilize the VPN tunnel. Agencies must be hosted or sponsored by a Collin County business department who will serve as the intermediary to complete any inter-local agreements or memorandums of understanding. Agencies must also complete Appendix B – VPN Tunnel Connection Document and submit the completed document to the Collin County Information Technology department via the sponsoring county department.

**NOTE: The option to access Collin County networks via a VPN tunnel is generally limited to law enforcement agencies who have complied with this policy. VPN tunnel access for non-law enforcement entities MUST be approved by the Collin County CIO and/or Commissioner's Court.**

By requesting access to the Collin County network via a VPN tunnel, agencies agree that they shall be bound by the following conditions:

1. Provide appropriate Cisco VPN equipment to establish and support the VPN tunnel from the agency network.
    a. Provide a Cisco ASA5510s, or equivalent Cisco device, to connect to the Collin County network(s) via a VPN tunnel.
    b. Provide resources to properly configure the equipment to connect to the VPN tunnel without assistance from Collin County beyond connection information included in this policy.
    c. Provide required resources for ongoing support of any client side VPN connection equipment.
2. Provide an accurate and completed Attachment B – VPN Tunnel Connection Document.
    a. Devices allowed through the VPN tunnel must be specified by the following:
        i. IP Address
            1. Requests to submit an IP address range or ranges will be addressed on a case by case basis.
        ii. Function/Purpose
        iii. Protocol
    b. Broad ranging access to the VPN tunnel from the entities network will not be allowed
        i. Access will only be granted to authorized functions and/or users.
3. It is the responsibility of the entity and/or user with VPN privileges to install, configure and setup their systems to connect to Collin County based on the information provided to them.
4. Ensure that access to the VPN tunnel will be managed, monitored and secured from within the agency network.
    a. Agency personnel will be trained that connection credentials, user accounts and passwords shall not be shared.
5. Access only the Collin County systems(s)/service(s) requested in Attachment B in support of authorized functions.
    a. External agencies, and any sponsoring Collin County department, requesting VPN tunnel access are responsible for defining what services and/or equipment the agency will access. **Access will be restricted to only those defined objects.** Attempting to connect to or access any service or device not defined will be considered a violation of the Collin County VPN tunnel policy and may result in immediate withdrawal of the right to use the VPN tunnel.
    b. Remote desktop protocol (RDP) will not be available through this tunnel.
    c. Use of remote control software (ex. LogMeIn, GoToMyPC, WebEx, etc.) within the Collin County network, either through the VPN or over the internet unless specifically authorized by the IT department, is not allowed.

6. Access the Collin County VPN tunnel ***only*** from the specific IP address(es) and/or range(s) documented on Appendix B.
    a. Submit documentation of changes to IP address(es) and/or ranges accessing the VPN tunnel two weeks prior to implementation of the change.
7. Acknowledge that while actively connected to the Collin County VPN tunnel, only approved traffic to and from the remote PC over the VPN tunnel will be supported and all other traffic will be dropped.
    a. Connection to the VPN tunnel will be limited to only specific ports and protocols.
    b. Connection to the VPN tunnel is not a highly available resource and, in the event of an outage or other service disruption, regardless of the cause of the error, will be subject to service interruption until the county is able to restore connectivity during normal business hours.
        i. After hours support for the VPN tunnel is NOT provided by the county.
    c. Collin County reserves the right to perform maintenance on the county VPN systems at any time without any prior notice.
8. Ensure that all agency computers connected to Collin County services via the VPN tunnel use the most up-to-date anti-virus software from a reputable IT vendor including any personal computers owned by agency employees that have been requested to access the VPN tunnel. The anti-virus software must be updated with the latest definition files from that vendor and automated virus scans performed on the computer.
9. Ensure that all agency computers connected to Collin County services via the VPN tunnel are kept up to date with the latest security patches for their operating system and applications installed on the connecting system(s).
10. Require VPN tunnel users to comply with the Collin County acceptable use policy when accessing services through the VPN. A copy of the Collin County acceptable use policy may be obtained from the Collin County department sponsoring the VPN tunnel connection.
11. Upon termination of an agreement or contract with Collin County, or at the request of the Collin County staff, the entity must uninstall the VPN connection from their end point equipment.
12. 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
13. Prior to acquiring VPN access all users will be required to pass a background check.

**Access Request Process**

1. To obtain access to the VPN tunnel, the agency must be sponsored by a Collin County department and Collin County IT must agree this access to Collin County information systems does pose a threat to county operations. An authorized signatory from the agency must sign Appendix B – VPN Tunnel Connection Document, on behalf of all personnel who will connect to the VPN tunnel, agreeing to protect the security of the Collin County network.
2. The Collin County IT department may require that the county sponsor and the entity verify continued access to the VPN tunnel is required on an annual basis.

**Enforcement**

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

**Liability**

1. The agency 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 agency's connection to the County's networks.
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 county personnel may provide the evidence of such monitoring to law enforcement officials. Anyone using the system connects at their risk and assumes all responsibility for any possible damage to their equipment.

## 6.0 PROCEDURES

**To obtain access to a VPN tunnel the following steps will be followed:**

1. The agency must commit to only allow access to the VPN tunnel to authorized users within their network using only the VPN connection and only to connect to the systems/services specified in Appendix B. The use of products such as GotoMyPC, LogMeIn or other products that open connections from inside the network on an "always on" basis and which do not require Collin County user participation are prohibited from use.
2. The agency must be sponsored by a Collin County department who will facilitate the access request with the county IT department and the county IT department must agree this access is necessary. The agency must provide a signed copy of Appendix B – VPN Tunnel Connection Document agreeing to protect the security of the Collin County network. VPN expiration will be based on the contract length unless further time is requested at the time the tunnel is created.
3. An authorized employee of the agency must sign the "Connection Policy and Agreement Form" form on behalf of the agency employees agreeing to protect the security of the Collin County network.
4. The agency must supply a Cisco firewall/router to support the VPN tunnel connection. The agency must also provide all required programming and maintenance support for the equipment without assistance from Collin County.
5. The agency and sponsoring department will identify what services/equipment will be accessed through the VPN tunnel. Only that equipment or service will be allowed through the tunnel.

6. The sponsoring department will create a Collin County Service Desk work order ticket for this services request.
7. Upon completing the VPN tunnel the county IT department will communicate access details to the sponsoring department to be relayed to the agency.

## 7.0 REVISION HISTORY

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

| Date | Revision # | Description of Change |
|---|---|---|
| 11/14/2012 | 1.0 | Initial creation – Draft |
| 11/29/2012 | 2.0 | EAS review, comment and ratification |
| 12/10/2012 | 2.1 | Updated document with input from IT Management w/r/t non-law enforcement access to VPN tunnel |

## 8.0 INQUIRIES

Direct additional access inquiries and issues to the sponsoring department.

## 9.0 APPENDICES

### APPENDIX A – DEFINITION OF TERMS

| 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 responsibility for the liability clause of this document. |

| | |
|---|---|
| Sponsoring Department | Collin County department sponsoring the access request for a non-employee user to have access to Collin County services/equipment through the VPN. |

## APPENDIX B – VPN TUNNEL CONNECTION DOCUMENT

***NOTE: ALL DATA MUST BE PROVIDED***

| **Agency Information** | |
|---|---|
| Agency Name | |
| Address | |
| Point of Contact | |
| Phone Number | |
| Email Address | |
| Secondary Contact | |
| Phone Number | |
| Email Address | |
| **Sponsoring Department Information** | |
| Sponsoring Department | |
| Point of Contact | |
| Phone Number | |
| **Connection Purpose** | |
| | |
| **Tunnel Settings** | |
| Tunnel Termination IP Address | |
| VPN Encryption Settings | |
| **Connection Settings** *(separate multiple entries by commas)* | |
| Source IP Address(es) | |
| Destination IP Address(es) | |
| Destination Port(s) | |

***Submission of the VPN TUNNEL CONNECTION DOCUMENT shall bind the requesting agency to Collin County policy 033 - External Entity VPN Tunnel policy, on file with the Collin County IT department.***

| **Signatures** | | | |
|---|---|---|---|
| Agency Representative | | Collin County Sponsor | |
| Printed Name | | Printed Name | |
| Signature | | Signature | |
| Title | | Title | |
| Date | | Date | |