

INTERLOCAL DISPATCH SERVICES AGREEMENT

This agreement is entered into on the 17 day of September, 2018, by and between the Community ISD (the "School") and Collin County, a political subdivision of the State of Texas (the "County").

RECITALS

1. The County, through the Sheriff's Office, owns and operates communication facilities used in dispatching its law enforcement and emergency service personnel.
2. The School desires to obtain certain dispatch services from the County. Therefore, under the authority of Texas Government Code, Title 7, Interlocal Cooperation Act, Section 791 et seq., the parties agree as follows:

SECTION 1. DEFINITIONS

DISPATCH SERVICES. The term "Dispatch Services" means all services necessary for the Collin County Sheriff's Office to receive calls for law enforcement service within the School's jurisdiction and to dispatch the School's law enforcement personnel in response to such calls.

HOSTING SERVICES. The term "Hosting Services" means the County will store the School's data as it relates to dispatch services.

SECTION 2. TERM

2.01 TERM. The term of this agreement shall commence on October 1, 2018 and shall continue in full force and effect through September 30, 2019.

2.02 TERMINATION. Either party may terminate this agreement by giving ninety (90) days written notice to the other party.

SECTION 3. SERVICES

3.01 The County agrees to provide dispatch services through the Sheriff's

Office to the School in the same manner and under the same work schedule as such services are provided in the operation of the County's law enforcement personnel.

3.02 Hosting Services. The County agrees to provide Hosting Services to the School and that it will provide 95% uptime availability of the service as covered herein.

3.03 Scheduled Maintenance: The School hereby acknowledges that the County may, from time to time, perform maintenance service on the County network, with or without notice to the School, which may result in the unavailability of the County network.

Emergency maintenance and maintenance for which the County has not given the School notice in accordance with this Agreement shall not be deemed scheduled maintenance for purposes of this Agreement. The County will make every effort to notify the School prior to scheduled maintenance. Notice may be given in various forms including but not limited to email notice and/or phone call.

3.04 Hosted Data Ownership. The School shall have sole ownership of the School's hosted data and the County shall make no claim to ownership of School's hosted data.

3.05 Hosted Data Back Up. The County will back up the School's hosted data on a daily basis. All data backups will meet Criminal Justice Information Systems (CJIS) requirements. Every effort is made to ensure the reliability of the backed up data in the event that it would be necessary to restore a database. The County, however, makes no guaranties that the backed up database will be error free. Upon request, the County will provide to the School a current database backup that can be restored to an alternate location to verify the contents and confirm the quality of the backup. All services required to provide the School's data and/or verify data will be provided in accordance with the County's current rates.

3.06 Remote Access Agreement. For each user the City is required to complete and return **Attachment (A)**, Connection Policy and Agreement Form for remote access and return to County to the address in 9.02 item (C). No access will be given to user unless County has received a Remote Access Agreement.

SECTION 4. NONEXCLUSIVITY OF SERVICE PROVISION

The parties agree that the County may contract to perform services similar or identical to those specified in this agreement for such additional governmental or public entities as the County, in its sole discretion, sees fit.

SECTION 5. COMPENSATION

5.01 The dispatch service charges for FY2019 in the amount of \$5,260.00 shall be paid by the School in quarterly installments of \$1,315.00 during the term hereof.

The fees will be based on the fee schedule formulas adopted by Commissioners' Court on August 6, 2018 (Court Order No. 2018-628-08-06). In addition to the fee schedule, each radio registered on the system will be assessed an annual connection fee by Plano, Allen, Wylie, Murphy (PAWM) operators for access to their system. In FY2019, the fee will be \$108 per radio and may be updated annually by PAWM.

5.02 PAYMENT UPON EARLY TERMINATION. If this agreement is terminated prior to the conclusion of a three-month period for which a payment has been made pursuant to Section 5.01 of this agreement, the entire amount paid shall belong to the County without prorating, as liquidated damages to cover the County's anticipated costs for staffing and equipment to provide services hereunder.

5.03 SOURCE OF PAYMENT. The School agrees that payments that it is required to make under this agreement shall be made out of the School's current

revenues.

SECTION 6. CIVIL LIABILITY

6.01 Any civil liability relating to the furnishing of services under this agreement shall be the responsibility of the School. The parties agree that the County shall be acting as agent for the School in performing the services contemplated by this agreement.

6.02 The School shall hold the County free and harmless from any obligation, costs, claims, judgments, attorney's fees, attachments, and other such liabilities arising from or growing out of the services rendered to the School pursuant to the terms of this agreement or in any way connected with the rendering of said services, except when the same shall arise because of the willful misconduct or culpable negligence of the County, and the County is adjudged to be guilty of willful misconduct or culpable negligence by a court of competent jurisdiction.

SECTION 7. AMENDMENT

This agreement shall not be amended or modified other than in a written agreement signed by the parties.

SECTION 8. CONTROLLING LAW

This agreement shall be deemed to be made under, governed by, and construed in accordance with the laws of the State of Texas.

SECTION 9. NOTICES

9.01 FORM OF NOTICE. Unless otherwise specified, all communications provided for in this agreement shall be in writing and shall be deemed delivered, whether actually received or not, forty-eight (48) hours after deposit in the United States mail, first class, registered or certified, return receipt requested, with proper postage prepaid or immediately when delivered in person.

9.02 ADDRESSES. All communications provided for in this agreement shall

be addressed as follows:

(A) Collin County, to:
Purchasing Department
2300 Bloomdale #3160
McKinney, Texas 75071

(B) If to the School, to:

Finance/Accounts Payable
611 FM 1138 North
Nevada, TX 75173

(C) Collin County, Remote Access to:
Information Technology Department
2300 Bloomdale #3198
McKinney, Texas 75071

Or to such person at such address as may from time to time be specified in a notice given as provided in this Section 9. In addition, notice of termination of this agreement by the School shall be provided by the School to the County Judge of Collin County as follows:

The Honorable Keith Self
Collin County Judge
Collin County Administration Building
2300 Bloomdale Rd. Suite 4192
McKinney, Texas 75071

SECTION 10. CAPTIONS

The headings to the various sections of this agreement have been inserted for the convenient reference only and shall not modify, define, limit or expand the express provision of this agreement.

SECTION 11. COUNTERPARTS

This agreement may be executed in counterparts, each of which, when taken separately, shall be deemed an original.

SECTION 12. OBLIGATIONS OF CONDITION

All obligations of each party under this agreement are conditions to further performance of the other party's continued performance of its obligation under the agreement.

SECTION 13. EXCLUSIVE RIGHT TO ENFORCE THIS AGREEMENT

The County and the School have the exclusive right to bring suit to enforce this Agreement, and no party may bring suit, as a third-party beneficiary or otherwise, to enforce this agreement.

SECTION 14. PRIOR AGREEMENTS SUPERSEDED

This agreement constitutes the sole and only agreement of the parties hereto and supersedes any prior understanding or written oral agreements between the parties respecting the services to be provided under this agreement.

IN WITNESS WHEREOF, THE PARTIES HERETO HAVE EXECUTED THIS AGREEMENT AS OF THE DAY AND YEAR FIRST ABOVE WRITTEN.

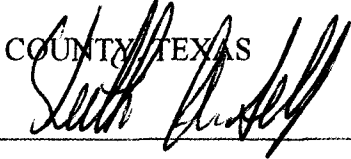
“COUNTY”

COLLIN COUNTY, TEXAS

BY: _____

TITLE: _____

DATE: _____



County Judge

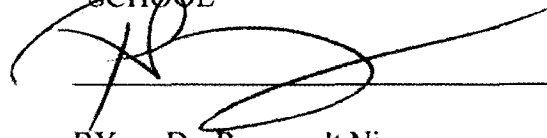
9/17/18

“SCHOOL”

BY: _____

TITLE: _____

DATE: _____



Dr. Roosevelt Nivens

Superintendent

8/30/18

Attachment "A"

Law Enforcement Officers Remote Connectivity Policy and Agreement Form

Remote Access Agreement

1.0 Purpose

The purpose of this document is to provide the framework for granting REMOTE ACCESS to Collin County services/equipment through REMOTE ACCESS so that an Authorized Party of a law enforcement agency (Agency) may access its data hosted on Collin County's network.

2.0 Scope

This policy applies to all Law Enforcement Officers utilizing REMOTE ACCESS to access the Collin County network (such persons referred to herein as "Authorized Parties"). This policy applies to all Collin County REMOTE ACCESS implementations.

3.0 Policy

Authorized parties may utilize the benefits of REMOTE ACCESS, which are a "user managed" service. This means that the Authorized party is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees as may be required to access the REMOTE ACCESS.

Additionally,

1. It is the responsibility of the Authorized Party 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 REMOTE ACCESS are responsible for defining what services/equipment/software 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 REMOTE ACCESS policy and will be reported to the Authorized Party's agency
3. The Authorized Parties and the Collin County employees sponsoring the REMOTE ACCESS request are also responsible for defining the time scope that the REMOTE ACCESS 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. REMOTE ACCESS 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 REMOTE ACCESS will force all traffic to and from the remote PC over the REMOTE ACCESS tunnel; all other traffic will be dropped.
6. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
7. REMOTE ACCESS gateways will be established and managed by Collin County Information Technology Department.
8. All computers connected to Collin County internal networks via REMOTE ACCESS or any other technology must use the most up-to-date anti-virus software from a reputable IT agency; this includes personal computers.
9. All Authorized Parties connecting to the Collin County internal networks via REMOTE ACCESS 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. All systems using REMOTE ACCESS connections to Collin County must comply with Microsoft's Product Lifecycle chart and use only currently supporting and fully patched operating systems.

10. Authorized Parties 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. Authorized Parties that are not Collin County owned equipment must comply with the Collin County acceptable use policy when accessing the Internet while connected through the REMOTE ACCESS.
12. Only approved REMOTE ACCESS clients may be used.
13. Upon termination of a contract from Collin County, or at the request of the Collin County staff, the Authorized Party must uninstall the REMOTE ACCESS connection from the Authorized Party's computer.
14. Agency expressly agrees to notify the County of staffing changes involving an Authorized Party with access to the County's network within 24 hours or next business day.
15. After six months of expired inactivity, Active Directory and REMOTE ACCESS accounts of an Authorized Party will be permanently deleted, unless otherwise approved by the County.
16. Accounts will be locked out after a certain number of failed attempts.
17. Authorized Parties who have lost their password will have to contact their sponsoring agency to request a password reset. The sponsoring agency will then contact Collin County IT to reset the password for the REMOTE ACCESS user. The sponsoring agency is the Sheriff's Office.
18. It is the responsibility of the Authorized Party to install, configure, setup and support any issues with their systems to connect to Collin County based on the information provided to them.
19. Authorized Parties connect at their own risk and Collin County is not responsible for any damages that they may incur from connecting through the REMOTE ACCESS to Collin County
20. Prior to acquiring REMOTE ACCESS all Authorized Parties will be required to pass a background check unless otherwise approved by the County.
21. If the County migrates to a new network connection technology it is the responsibility of the Agency to budget and obtain any required technology upgrade in order to maintain their network connection to the County. The Agency will be provided advance notification for this change.
22. The Authorized Party must notify Collin County IT immediately upon learning of any compromise occurring through an anti-virus, malware, or other form of unauthorized access. Collin County will also inform the Authorized Parties of any breach or suspected breach occurring on the county network. REMOTE ACCESS may be restricted during such an event while corrective actions are undertaken.

4.0 Granting Access

To obtain access via REMOTE ACCESS, the Agency and Authorized Party 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 Agency and Authorized Party must sign this form agreeing to protect the security of the Collin County network. For external Authorized Parties, the Request for REMOTE ACCESS must be signed and approved by the Manager who is responsible for the external Authorized Party's use. REMOTE ACCESS expiration will be based on the contract length unless further time is requested by Collin County Management.

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

5.0 Enforcement

Collin County Information Technology Department may actively monitor the REMOTE ACCESS concentrator for any suspicious and inappropriate activity. Any Authorized Party found to have violated any part of this policy may have their REMOTE ACCESS terminated immediately.

6.0 Liability

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, including that caused by their Authorized Parties, to the County’s services/equipment resulting from or related to Agency’s connection to the County’s networks.

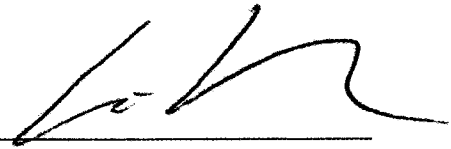
Unauthorized access or use is prohibited and will be prosecuted to the fullest extent. Anyone using this system expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personnel may provide the evidence of such monitoring to law enforcement 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
REMOTE ACCESS	An extension of Collin County’s internal private network.
REMOTE ACCESS Concentrator	Physical device that manages REMOTE ACCESS connections.
REMOTE ACCESS Client	Remote computer with REMOTE ACCESS software utilizing REMOTE ACCESS services.
Agency Management	Person in Agency company that can take responsibility for the liability clause of this document.
Dual (split) tunneling	When utilizing REMOTE ACCESS, 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 REMOTE ACCESS.
User	Employee, Agency, 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 REMOTE ACCESS.

The employee may be someone in IT.

Agency Management's Signature (if applicable)

Printed Name: Scotty Morrison, Chief of Police Signature: 

E-Mail Address: scotty.morrison@communityisd.org Phone: 972-843-6060 Date: 8/28/18

Remote Access Users Signature

Printed Name: Scotty Morrison Signature: 

E-Mail Address: scotty.morrison@communityisd.org Phone: 972-843-6060 Date: 8/28/18

Sponsoring Party's Signature

Printed Name: _____ Signature: _____

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

Return form to:

Caren Skipworth
2300 Bloomdale #3198
McKinney, Texas 75071

Attachment "A"

Law Enforcement Officers Remote Connectivity Policy and Agreement Form

Remote Access Agreement

1.0 Purpose

The purpose of this document is to provide the framework for granting REMOTE ACCESS to Collin County services/equipment through REMOTE ACCESS so that an Authorized Party of a law enforcement agency (Agency) may access its data hosted on Collin County's network.

2.0 Scope

This policy applies to all Law Enforcement Officers utilizing REMOTE ACCESS to access the Collin County network (such persons referred to herein as "Authorized Parties"). This policy applies to all Collin County REMOTE ACCESS implementations.

3.0 Policy

Authorized parties may utilize the benefits of REMOTE ACCESS, which are a "user managed" service. This means that the Authorized party is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees as may be required to access the REMOTE ACCESS.

Additionally,

1. It is the responsibility of the Authorized Party 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 REMOTE ACCESS are responsible for defining what services/equipment/software 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 REMOTE ACCESS policy and will be reported to the Authorized Party's agency
3. The Authorized Parties and the Collin County employees sponsoring the REMOTE ACCESS request are also responsible for defining the time scope that the REMOTE ACCESS 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. REMOTE ACCESS 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 REMOTE ACCESS will force all traffic to and from the remote PC over the REMOTE ACCESS tunnel; all other traffic will be dropped.
6. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
7. REMOTE ACCESS gateways will be established and managed by Collin County Information Technology Department.
8. All computers connected to Collin County internal networks via REMOTE ACCESS or any other technology must use the most up-to-date anti-virus software from a reputable IT agency; this includes personal computers.
9. All Authorized Parties connecting to the Collin County internal networks via REMOTE ACCESS 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. All systems using REMOTE ACCESS connections to Collin County must comply with Microsoft's Product Lifecycle chart and use only currently supporting and fully patched operating systems.

10. Authorized Parties 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. Authorized Parties that are not Collin County owned equipment must comply with the Collin County acceptable use policy when accessing the Internet while connected through the REMOTE ACCESS.
12. Only approved REMOTE ACCESS clients may be used.
13. Upon termination of a contract from Collin County, or at the request of the Collin County staff, the Authorized Party must uninstall the REMOTE ACCESS connection from the Authorized Party's computer.
14. Agency expressly agrees to notify the County of staffing changes involving an Authorized Party with access to the County's network within 24 hours or next business day.
15. After six months of expired inactivity, Active Directory and REMOTE ACCESS accounts of an Authorized Party will be permanently deleted, unless otherwise approved by the County.
16. Accounts will be locked out after a certain number of failed attempts.
17. Authorized Parties who have lost their password will have to contact their sponsoring agency to request a password reset. The sponsoring agency will then contact Collin County IT to reset the password for the REMOTE ACCESS user. The sponsoring agency is the Sheriff's Office.
18. It is the responsibility of the Authorized Party to install, configure, setup and support any issues with their systems to connect to Collin County based on the information provided to them.
19. Authorized Parties connect at their own risk and Collin County is not responsible for any damages that they may incur from connecting through the REMOTE ACCESS to Collin County
20. Prior to acquiring REMOTE ACCESS all Authorized Parties will be required to pass a background check unless otherwise approved by the County.
21. If the County migrates to a new network connection technology it is the responsibility of the Agency to budget and obtain any required technology upgrade in order to maintain their network connection to the County. The Agency will be provided advance notification for this change.
22. The Authorized Party must notify Collin County IT immediately upon learning of any compromise occurring through an anti-virus, malware, or other form of unauthorized access. Collin County will also inform the Authorized Parties of any breach or suspected breach occurring on the county network. REMOTE ACCESS may be restricted during such an event while corrective actions are undertaken.

4.0 Granting Access

To obtain access via REMOTE ACCESS, the Agency and Authorized Party 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 Agency and Authorized Party must sign this form agreeing to protect the security of the Collin County network. For external Authorized Parties, the Request for REMOTE ACCESS must be signed and approved by the Manager who is responsible for the external Authorized Party's use. REMOTE ACCESS expiration will be based on the contract length unless further time is requested by Collin County Management.

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

5.0 Enforcement

Collin County Information Technology Department may actively monitor the REMOTE ACCESS concentrator for any suspicious and inappropriate activity. Any Authorized Party found to have violated any part of this policy may have their REMOTE ACCESS terminated immediately.

6.0 Liability

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, including that caused by their Authorized Parties, to the County’s services/equipment resulting from or related to Agency’s connection to the County’s networks.

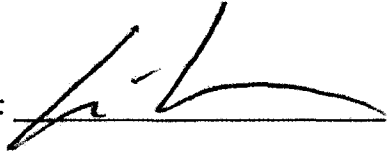
Unauthorized access or use is prohibited and will be prosecuted to the fullest extent. Anyone using this system expressly consents to monitoring and is advised that if such monitoring reveals possible evidence of criminal activity system personnel may provide the evidence of such monitoring to law enforcement 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
REMOTE ACCESS	An extension of Collin County’s internal private network.
REMOTE ACCESS Concentrator	Physical device that manages REMOTE ACCESS connections.
REMOTE ACCESS Client	Remote computer with REMOTE ACCESS software utilizing REMOTE ACCESS services.
Agency Management	Person in Agency company that can take responsibility for the liability clause of this document.
Dual (split) tunneling	When utilizing REMOTE ACCESS, 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 REMOTE ACCESS.
User	Employee, Agency, 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 REMOTE ACCESS.

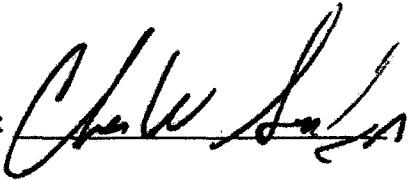
The employee may be someone in IT.

Agency Management's Signature (if applicable)

Printed Name: Scotty Morrison, Chief of Police Signature: 

E-Mail Address: scotty.morrison@communityisd.org Phone: 972-843-6060 Date: 8/28/18

Remote Access Users Signature

Printed Name: Chuck Sibley Signature: 

E-Mail Address: chuck.sibley@communityisd.org Phone: 972-843-6061 Date: 8/28/18

Sponsoring Party's Signature

Printed Name: _____ Signature: _____

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

Return form to:

Caren Skipworth
2300 Bloomdale #3198
McKinney, Texas 75071

Attachment "A"

Law Enforcement Officers Remote Connectivity Policy and Agreement Form

Remote Access Agreement

1.0 Purpose

The purpose of this document is to provide the framework for granting REMOTE ACCESS to Collin County services/equipment through REMOTE ACCESS so that an Authorized Party of a law enforcement agency (Agency) may access its data hosted on Collin County's network.

2.0 Scope

This policy applies to all Law Enforcement Officers utilizing REMOTE ACCESS to access the Collin County network (such persons referred to herein as "Authorized Parties"). This policy applies to all Collin County REMOTE ACCESS implementations.

3.0 Policy

Authorized parties may utilize the benefits of REMOTE ACCESS, which are a "user managed" service. This means that the Authorized party is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees as may be required to access the REMOTE ACCESS.

Additionally,

1. It is the responsibility of the Authorized Party 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 REMOTE ACCESS are responsible for defining what services/equipment/software 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 REMOTE ACCESS policy and will be reported to the Authorized Party's agency.
3. The Authorized Parties and the Collin County employees sponsoring the REMOTE ACCESS request are also responsible for defining the time scope that the REMOTE ACCESS 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. REMOTE ACCESS 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 REMOTE ACCESS will force all traffic to and from the remote PC over the REMOTE ACCESS tunnel; all other traffic will be dropped.
6. Dual (split) tunneling is NOT permitted; only one network connection is allowed.
7. REMOTE ACCESS gateways will be established and managed by Collin County Information Technology Department.
8. All computers connected to Collin County internal networks via REMOTE ACCESS or any other technology must use the most up-to-date anti-virus software from a reputable IT agency; this includes personal computers.
9. All Authorized Parties connecting to the Collin County internal networks via REMOTE ACCESS 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. All systems using REMOTE ACCESS connections to Collin County must comply with Microsoft's Product Lifecycle chart and use only currently supporting and fully patched operating systems.

10. Authorized Parties 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. Authorized Parties that are not Collin County owned equipment must comply with the Collin County acceptable use policy when accessing the Internet while connected through the REMOTE ACCESS.
12. Only approved REMOTE ACCESS clients may be used.
13. Upon termination of a contract from Collin County, or at the request of the Collin County staff, the Authorized Party must uninstall the REMOTE ACCESS connection from the Authorized Party's computer.
14. Agency expressly agrees to notify the County of staffing changes involving an Authorized Party with access to the County's network within 24 hours or next business day.
15. After six months of expired inactivity, Active Directory and REMOTE ACCESS accounts of an Authorized Party will be permanently deleted, unless otherwise approved by the County.
16. Accounts will be locked out after a certain number of failed attempts.
17. Authorized Parties who have lost their password will have to contact their sponsoring agency to request a password reset. The sponsoring agency will then contact Collin County IT to reset the password for the REMOTE ACCESS user. The sponsoring agency is the Sheriff's Office.
18. It is the responsibility of the Authorized Party to install, configure, setup and support any issues with their systems to connect to Collin County based on the information provided to them.
19. Authorized Parties connect at their own risk and Collin County is not responsible for any damages that they may incur from connecting through the REMOTE ACCESS to Collin County
20. Prior to acquiring REMOTE ACCESS all Authorized Parties will be required to pass a background check unless otherwise approved by the County.
21. If the County migrates to a new network connection technology it is the responsibility of the Agency to budget and obtain any required technology upgrade in order to maintain their network connection to the County. The Agency will be provided advance notification for this change.
22. The Authorized Party must notify Collin County IT immediately upon learning of any compromise occurring through an anti-virus, malware, or other form of unauthorized access. Collin County will also inform the Authorized Parties of any breach or suspected breach occurring on the county network. REMOTE ACCESS may be restricted during such an event while corrective actions are undertaken.

4.0 Granting Access

To obtain access via REMOTE ACCESS, the Agency and Authorized Party 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 Agency and Authorized Party must sign this form agreeing to protect the security of the Collin County network. For external Authorized Parties, the Request for REMOTE ACCESS must be signed and approved by the Manager who is responsible for the external Authorized Party's use. REMOTE ACCESS expiration will be based on the contract length unless further time is requested by Collin County Management.

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

5.0 Enforcement

Collin County Information Technology Department may actively monitor the REMOTE ACCESS concentrator for any suspicious and inappropriate activity. Any Authorized Party found to have violated any part of this policy may have their REMOTE ACCESS terminated immediately.

6.0 Liability

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, including that caused by their Authorized Parties, to the County’s services/equipment resulting from or related to Agency’s connection to the County’s networks.

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.

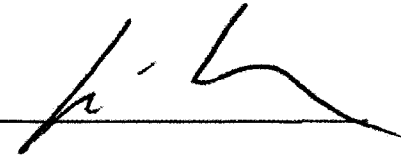
7.0 Definitions

Term	Definition
REMOTE ACCESS	An extension of Collin County’s internal private network.
REMOTE ACCESS Concentrator	Physical device that manages REMOTE ACCESS connections.
REMOTE ACCESS Client	Remote computer with REMOTE ACCESS software utilizing REMOTE ACCESS services.
Agency Management	Person in Agency company that can take responsibility for the liability clause of this document.
Dual (split) tunneling	When utilizing REMOTE ACCESS, 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 REMOTE ACCESS.
User	Employee, Agency, 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 REMOTE ACCESS.

The employee may be someone in IT.

Agency Management's Signature (if applicable)

Printed Name: Scotty Morrison, Chief of Police Signature: _____

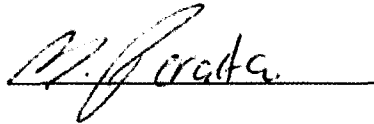


E-Mail Address: scotty.morrison@communityisd.org Phone: 972-843-6060 Date: 8/28/18

Remote Access Users Signature

Printed Name: Maria Peralta

Signature: _____



E-Mail Address: maria.peralta@communityisd.org Phone: 972-843-6062 Date: 8/28/18

Sponsoring Party's Signature

Printed Name: _____ Signature: _____

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

Return form to:

Caren Skipworth
2300 Bloomdale #3198
McKinney, Texas 75071