



Louisville Metro Technology Services – Remote Access Request Form

5.0 Remote Access/VPN Policy

5.1 Overview

Remote access/VPN technology (Virtual Private Network) allows Louisville Metro Government employees and affiliates connect to the Louisville Metro Government network via the Internet in a secure manner. This provides the ability to work from home and other locations not directly connected to the Louisville Metro Government network.

5.2 Purpose

The purpose of this policy is to define standards for connecting to the Louisville Metro Government's network from any host outside the network. These standards are designed to minimize the potential exposure to the Louisville Metro Government from damages, which may result from unauthorized use of Louisville Metro Government technology resources. Damages include the loss of sensitive or organizational confidential data, intellectual property, damage to public image, damage to critical Louisville Metro Government internal systems, etc.

5.3 Scope

This policy applies to all Metro Government employees, contractors, temporary workers, vendors, agencies, and agents requesting access to Metro Government resources. This policy applies to remote access conditions used to do work on behalf of the Louisville Metro Government, including reading or sending of email, files, vendor support, viewing Intranet web resources and in times of emergencies.

It also applies to the use of Louisville Metro Government owned PC's that are computer connected to the Louisville Metro Government network via DSL through VPN.

Remote access implementations that are covered by this policy include, but are not limited to wireless, dial-in modems, frame relay, PGP, ISDN, SSL, DSL, IPSEC, SSH, FTP, SFTP, VPN, Terminal Services and cable modems.

5.4 Policy

5.4(1) General

- It is the responsibility of Metro Government employees and affiliates with remote access privileges to the Metro Government's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Metro Government resources.
- General access to the Internet for recreational use via a Louisville Metro Government remote access account by immediate household members through the Metro Government is forbidden.
- All Louisville Metro Government IT Security Policies apply to remote access accounts and usage.
- All persons having signature authority for approving remote access will be aware that there are costs associated with and security risks involved with persons having the ability to access Metro-owned network resources remotely. Approval will only be granted if there are significant business reasons to do so.
- Metro Government primary means for remote connectivity is SSL VPN through a web browser.
- When there is a business requirement to transfer large files in and out of the Louisville Metro Government network it will be encrypted and transmitted through Secure File Transfer Protocol (SFTP) or PGP to ensure its integrity and security.

Any and all costs associated with accessing the Louisville Metro Government's resources remotely are the responsibility of the requesting department. Costs may include, but are not limited to, costs associated with procurement of a computer, Internet Service Provider (ISP) costs, licenses, etc. The department manager will determine what costs the agency will absorb and what costs, if any, the remote user will incur for this service. Metro Technology Services is not responsible for absorbing any costs associated with employees and affiliates accessing the Metro Government's resources remotely.



Louisville Metro Technology Services – Remote Access Request Form

5.4(1a) Digital Subscriber Line Connections

This section applies to Louisville Metro Government Agencies that connect to our internal network through DSL connections through VPN and agencies that require or provide personal computers to the public for Internet or general usage.

When in implementation, all personal computers connected in this manner while follow the guidelines set in all Louisville Metro Government Information Security Policies. Metro Technology Services must have the ability to centrally manage the computers.

5.4(2) Requirements

- A “[Remote Access Request Form](#)” must be submitted to Metro Technology Services prior to remote access privileges being granted (except for DSL through VPN connections).
- Secure remote access must be strictly controlled. User ID’s/ passwords will be assigned by Metro Technology Services.
- At no time will any Louisville Metro Government employee or affiliate provide his/her login password or account to anyone, not even family members.
- Louisville Metro Government employees and affiliates with remote access privileges must ensure that their company-owned or personal computer or workstation, which is remotely connected to the Louisville Metro Government’s corporate network, has properly installed anti-virus software utilizing current anti-virus detection definitions, management software and current operating system and application security patches installed.
- Reconfiguration of a home user’s equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
- When remote access is no longer required, it is the department’s (sponsor) responsibility to notify Metro Technology Services so access can be terminated.
- Organizations/ personnel who wish to implement non-standard remote access solutions to the Louisville Metro Government production network must obtain prior approval from Metro Technology Services.
- Remote access users must read all messages sent from Metro Technology Services regarding remote access.

5.5 Enforcement

Any employee/affiliate found to have violated this policy will be subject to termination of remote access, disciplinary action, up to and including termination of employment.

5.6 Revisions

03-01-04 Original
06-24-04 Revised
07-19-04 Revised
09-29-04 Revised
01-20-05 Revised
12-17-07 Revised
03-25-08 Revised
06-27-08 Revised



Louisville Metro Technology Services – Remote Access Request Form

Section I – User Information						
Agency/Vendor Name		Department		Division (if applicable)		
Agency/Vendor Address		City		Zip Code		
Applicant's Name	Last	First	Middle Initial			
Contact Information	Phone #		Email Address			
Section II – Detailed Explanation of Request						
<i>What will you be connecting to (server, application, etc.)? Do you have any unique requirements? Have accounts been created on the appropriate internal systems? Describe the work to be completed.</i>			<i>The more detailed information we receive, the faster the request can be completed.</i>			
Section III – Type of access being requested:						
<i>Metro Technology Services' primary means of remote access is SSL/VPN through a web browser; all other means must be pre-approved by Metro Technology Services.</i>		SSL/VPN <input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Remove	RDP/TS <input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Remove	SSH <input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Remove	SFTP <input type="checkbox"/> New <input type="checkbox"/> Update <input type="checkbox"/> Remove	Other - Please Specify
Section IV – Vendor/Contract Agency Request Remote Access						
<i>If the request is for non-SSL VPN connectivity, a static public IP address must be supplied.</i>			Static IP Address			
Section V – Authorization						
<i>The form must be signed by the requestor's Director (or authorizing Metro Government Director for access)</i>			By signing this document, <ul style="list-style-type: none"> I have read and understand the Louisville Metro Government Remote Access Policy I understand that Metro Technology Services will audit usage of remote access accounts to verify compliance and use Failure to comply with Louisville Metro Government Information Security Policies will result in immediate termination of remote access. I understand it is my responsibility to read all email communications regarding system status, updates and other information pertaining to Louisville Metro remote access I understand I will not be allowed to connect unless the computer I am using is up to date on antivirus and current operating system patches are installed 			
Applicant's signature:					Date	
Remote Access Authorized by (Director/Sponsor):			Print name of authorizing signature		Signature	
Title of authorizing signature:					Phone:	
Submit completed forms to the Metro Technology Services via fax (502) 574-4329. Completed and approved forms will be processed within five business days after receipt. Metro Technology is not responsible for delays in granting access due to errant or incomplete information.						
For Information Technology Services Use Only						
Date received:	It Security Sign-Off:	Assyst ticket number:	Approving MTS Director:			