

Metro Government Information Technology Environment Overview and Expectations for Technology Vendor Submissions

Prepared by Information Technology Service (ITS)

Revised January 6, 2026

The following technologies are used to support public services offered by more than fifty departments and agencies of the Metropolitan Government of Nashville & Davidson County, Tennessee (Metro). The purpose of this document, as authored by Metro Information Technology Services Department (ITS), is to inform potential vendors of the information technology environment their proposed solution must work within and to identify Metro Government preferences and expectations based on that environment, in consideration of existing costs, expertise, supportability and maintenance contracts.

Authentication

Microsoft Active Directory (AD) is Metro's central authentication for access to email, printers, directories, files, and most applications. Maintaining the user IDs, passwords and associated rights of AD is an ongoing task involving staff time and procedural checks and balances to ensure that all security risks are mitigated. Similar effort and attention are needed for any additional list of accounts and access rights on the network.

It is therefore in the best interests of Metro from the perspectives of both cost and security, that any proposed vendor solution must use Metro's existing AD accounts as the source for single sign on functionality and rights or provide "pass-through" authentication to those accounts and rights using Metro's existing AD accounts, rather than requiring separate account maintenance and user authentication. Metro also maintains AD Federated Services (ADFS) for authentication.

Vendor proposed solutions must be robust enough to handle user accounts from multiple peer domains and multiple forests.

Server and Client

Metro ITS's support infrastructure is primarily built around Microsoft Windows clients using both Windows and Linux based servers. RHEL (RedHat) is our approved Linux operating system unless a solution is an appliance/turnkey package. Virtual machines are the standard build for servers, but not yet for clients. For cloud hosted solutions, Microsoft Azure is the preferred IaaS provider.

For application access, browser-based thin clients are strongly preferred. The use of thick clients must include the frequency, detailed procedures and estimated time required for client updates.

Proposed solutions requiring either cloud-based, external server hosting or the use of software such as the LAMP (Linux, Apache, MySQL, and Perl) platform or variants, must include detailed documentation regarding the areas described in this document (account maintenance, security patching, backups and restores, etc.).

Database

Within Metro Microsoft SQL is more commonly used in Metro than Oracle, and is the clear preference from cost, installation, and support perspectives. That said, some Metro departments maintain significant existing Oracle installations and will prefer the use of Oracle database for software that a particular department will support. Oracle database installations can be either cloud hosted or hosted on premise with physical hardware.

Vendors proposing solutions that use a database should ask whether SQL or Oracle is preferred for that solution. Vendors proposing solutions that use a database other than SQL or Oracle must explain how ongoing maintenance tasks such as patching, backup, recovery, re-indexing or deleted-space compacting will be handled and how much time those tasks will take on an ongoing basis, along with how initial and ongoing licensing will be purchased.

Patching

Metro has an aggressive patch management process for Microsoft operating systems/Office applications for both clients and servers. If vendor systems or applications require a significant waiting period past the Microsoft patch release(s) date, the vendor must explain how security concerns will be addressed while the system is in a more vulnerable state.

Similar processes and concerns apply to Metro's support and patching of the Linux Server Operating System. Testing is done prior to installation. Application security patches (Adobe Reader, IIS, SQL, etc.), are also deployed in a timely manner after release by the manufacturer. Any dependencies on client-side software (JAVA, Adobe, web browsers, etc.) should be fully documented. If vendor systems or applications require a significant waiting period past the releases date(s) of these patches, the vendor must explain how security concerns will be addressed while the system is in a more vulnerable state. If system patching is to be handled by Metro, then special requirements for testing patches and updates should be fully documented and provided to ITS for review.

If system patching is to be handled by the vendor as part of a "turnkey" system, then the patching process must be fully documented and provided to Metro ITS for review. This process should include how quality assurance is addressed and should include the handling of any "out of band" patches or patches to address "zero day" vulnerabilities that are being actively exploited. Any modifications, updates, etc., that will cause a disruption of services must be scheduled with the Metro point of contact for the system.

Backup and Recovery

Metro policy requires all proposed systems to include a backup and restoration solution. All vendor proposed solutions must provide complete and detailed documentation on the backup and recovery of the proposed system. Vendor shall be willing to state usual mean time to recovery (MTR) numbers for the services that they provide and shall describe how any backups of Metro data are going to be handled and what the security controls around those backups would be.

Security

All proposed solutions must comply with Metro security policies. Current Metro Information security policies may be found at <https://www.nashville.gov/departments/information-technology-services/information-security/doing-it-business-metro>

Entities that desire to do any of the following are required to complete the Metropolitan Government's Information Security Agreement Questionnaire [MISA-Questionnaire V1 9.pdf \(nashville.gov\)](#) :

- provide software or hardware to Metro
- connect to the Metro network
- provide services over a network (i.e. cloud-bases services, etc.)
- access or store Metropolitan Government department or agency data

Metro manages firewalls to maintain the security of the Metro network, both host-based and network. Any vendor-proposed solution should provide detailed documentation on what ports and/or protocols are used by the application for communication. Metro prefers the use of standard ports for any communications. Any nonstandard ports used by a solution should be fully explained. The protocols and direction of the flow of traffic should also be provided.

Vendor-proposed solution(s) and/or application(s) should be able to work with encryption utilizing NIST-approved encryption algorithms and provide a means to ensure the security of the application and the data the proposed solution handles or stores.

Metro requires all PCs and servers to maintain active and daily updated antivirus software, currently provided through contract with Trend Micro. Blocking of standard executable attachments and exploits occurs at the enterprise level through Microsoft Exchange as well as other common connection points and some intrusion detection software. If a vendor has concerns regarding this, additional detail can be provided upon request, on a limited and confidential basis.

Outside connectivity to the Metro network is through VPN only. Metro does not allow the use of remote access tools, such as PCAnywhere.

Metro practices “least privilege” with regards to access. Solutions or applications should not require users to have administrative or high-level permissions to servers or desktops in order to function properly. While such permissions may be required for initial installation of the application, it should not be needed to run the application.

User access and the open security ports needed for applications to communicate must be clearly defined before any system is to be installed.

Metro performs both operating and application vulnerability scanning against all solutions prior to solutions being moved into production. Vendor is required to address all identified Critical, High, or Medium vulnerabilities by either correcting the vulnerability or determining an acceptable method of remediation.

Encryption may be required before certain data can be transferred or stored and malfunctioning or end-of-life devices containing sensitive data must be surrendered to Metro for destruction. Specific questions will be answered, and documents provided upon request. If an encryption solution is used, then proof must be provided showing the cryptographic module used for encryption is on the National Institute of Standards and Technology’s (NIST’s) Cryptographic Module Validation Program (CMVP) list at <http://csrc.nist.gov/groups/STM/cmvp/validation.html#01>.

Development Environment

The current development environment within ITS is:

- a) SQL Server / Oracle Database (multiple versions)
- b) Microsoft Visual Studio Development Tools primarily using C#, C++ & ASP.NET.
- c) Power Platform
- d) JSON, XML, XSLT, CSS, and JavaScript.
- e) IIS v8.0 or later
- f) Data models, programming using TSQL, data transformation services (DTS /SSIS).
- g) Standard project methodology through the entire project life cycle that includes the use of appropriate security controls.

Network Environment

Metro has deployed an Enterprise network built on a Cisco Systems foundation. All devices on the internal network are addressed with a private IPv4 address. Metro requires vendors to provide details of physical connection requirements to include media type and connection speeds. Metro additionally requires vendor to provide details of the solutions logical communication requirements to include specific network protocols with port number(s)

used between devices, source, and destination points of communication, and identify any communication that occurs outside of the Metro Enterprise network.

The following are minimum requirements for connecting to the Metro Enterprise network:

- a) All network communications devices will be managed by ITS and purchased through ITS.
- b) All devices will be configured to use Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS)
- c) All devices must be capable of communicating across a layer 3 network. Layer 2 only requirements must be pre-approved
- d) Multicast communications are not typically allowed and therefore require pre-approval
- e) All network communication devices will be provided by ITS unless pre-approved by ITS. "Network Communication devices" includes any device that is responsible for carrying IP packets to an endpoint or client and can include but is not limited to switches, routers, hubs, firewalls, media convertors, wireless devices, etc.

Artificial Intelligence (AI)

The Metropolitan Government of Nashville and Davidson County (Metro) understands the benefits of Artificial Intelligence (AI) to improve the delivery of services to residents. At the same time, we understand the concerns residents have with these solutions as well as the need to address information security and data privacy obligations.

Metro's AI Mission: To efficiently, securely and ethically implement trustworthy AI systems that improve the delivery of services to the residents of the Metropolitan Government of Nashville and Davidson County.

Metro seeks to ensure that Metro's AI-powered technology acquisitions perform accurately, minimize bias, are reliable and meets Metro's guiding Responsible AI goals:

- **Accountability:** to ensure AI systems have a human owner responsible for system oversight, accountability and measuring accuracy.
- **Accuracy:** to deploy AI systems that have a high accuracy rate.
- **Equity:** to use AI in alignment with Metro's commitment to equity and reducing racial and socioeconomic disparities.
- **Security:** to ensure appropriate security and data privacy is provided in all AI systems.
- **Transparency:** to provide information about the AI systems it uses to the general public so that they are informed.
- **Utility:** to adopt AI systems that will have a useful and positive impact on residents and the delivery of services.

Any Artificial Intelligence (AI) solution, whether stand alone or a solution embedded with or using AI within its software or service offering, must undergo an ITS led risk assessment prior to purchase or implementation.

Summary of Environment

Metro's commonly supported environment includes the products listed below. Backward compatibility stance for all proposed solutions should be provided. Upon completion of contract, specific versions or release numbers of tools will be provided under NDA.

PRODUCT	FUNCTION
Microsoft Active Directory Services	Central list of users and IDs that governs access to Metro data, printers, servers, and applications. Metro supports multiple forests and multiple peer domains in those forests.
Microsoft Active Directory Federated Services	Solution for federating identity with external sources.
Exchange Online as part of Microsoft 365	Central email platform supports only MAPI.
SharePoint Online	Team, project, or group level file storage, sharing and collaboration.
One Drive for Business	Individual user level file storage, sharing and collaboration.
Microsoft Power Platform	Power Apps and Power Automate for new tools and automation initiatives
Microsoft Windows Standard Server OS, 2022, 2019, 2016, 2012 R2. Red Hat Linux 6.6 or above.	Server Operating Systems.
Microsoft Windows Windows 11	Desktop Operating System
Dell PowerEdge and Blade Hardware, UCS Platform	Hardware for servers.
Dell Hardware for both PCs and laptops. Panasonic Toughbook for ruggedized laptops.	Hardware for PCs
Microsoft IIS v8.0 or later	Internet and Intranet hosting software.
Microsoft SQL Server	Enterprise database software.
Oracle Application Server and some major Oracle databases	Enterprise database software

PRODUCT	FUNCTION
Dell EMC PowerStore and PowerScale SAN-attached storage	Shared Storage Area Network hardware SAN use is preferable over direct attached storage.
CommVault	Server backup software.
CrowdStrike, Trend Micro OfficeScan/APEX one	Desktop and server antivirus software
Microsoft System Center Operations Manager 2012 R2 UR14	Enterprise monitoring and alerting software.
Microsoft Configuration Manager version 2503	Enterprise hardware and software inventory, application deployment, Microsoft updates deployment and Windows operating system deployments.
Microsoft System Center Orchestrator 2022	Enterprise workflow automation software.
VMware vSphere 6.7	Server virtualization software.
Cisco Routers and Switches	Network hardware and software.
Cisco phone equipment	VoIP hardware and software.
Cisco Webex	Conferencing, Messaging, and Softphone client
Cisco Wireless LAN Controllers and Access Points	Wireless Infrastructure Management
Microsoft Edge, Chrome	Internet browser
Checkpoint Endpoint Security VPN or Cisco AnyConnect VPN	Client VPNs
Checkpoint	Site-to-site VPN
ForcePoint	URL Filtering solution
F5 Big IP Local Traffic Manager (LTM)	Application Load Balancing, Reverse Proxy
Esri ArcGIS Server 11.3 or later	Enterprise GIS Platform
Milestone Corporate Video Management System	Enterprise Video Management System

Lenel OnGuard	Enterprise Access Control System
---------------	----------------------------------

For questions, please contact the Metro ITS Service Desk at ITSHelpdesk@nashville.gov.