RFP 7976-0-2020/ML
Integrated Security System for the Juvenile Detention Center

ATTACHMENT I: TECHNOLOGY AN DENVIRONMENT STANDARDS

The City's Department of Information Technology (IT) reviews and updates the standards of acceptable and supported computers, printers, servers, network equipment, database management systems, telephony equipment, application systems and software on an on-going basis. Guidelines and preferred standards as of the issue date of this RFP are listed below.

Hosted and Cloud-Based Applications and Databases

- All datacenters for cloud-based or hosted applications and storage must reside within the contiguous United States. City of Norfolk data shall not be stored outside the contiguous United States.
- All City of Norfolk data used, input, updated or modified in the system is the sole property of the City of Norfolk and can be used by Norfolk staff or designated agents for any purpose.
- Data hosted in cloud services must be accessible by standard web protocols such as REST and SOAP APIs.
- All servers must be running the RSA SecurID GINA and all personnel with Administrator rights must be issued an RSA hardware or software token. Alternate multi-factor authentication could be used if it is managed and controlled by City of Norfolk's Network/Security staff.
- Site to site Virtual Private Network (VPN) connections for cloud-based applications will be reviewed on a case-by-case basis.
- Web applications must be certified to work with high encryption for HTTPS traffic and support only TLS 1.2 encryption protocols. Group policies will be created to enforce this on servers and computers. Standalone systems, such as DMZ servers, will be performed manually.
- Vendors should not install backdoor or administrative accounts on the servers, applications or databases without providing all credentials to the City IT Security staff.
- No unchangeable hardcoded credentials shall be on applications. All credentials must be changeable by City staff at any time for any reason without negatively impacting application functionality.
- Vendors must safeguard the provided credentials to any City or external system configured for the City and must not share the credentials with anyone else. Should vendor suspect the credentials are compromised, it must communicate this immediately to the City's point of contact.
- Creation of Cloud services without IT involvement and approval in advance is discouraged and may not be supported. City of Norfolk staff have the right to disable or remove access to such services due to security concerns or compliance regulation violations.
- All datacenters for cloud-based or hosted applications and storage must reside within the contiguous United States. City of Norfolk data shall not be stored outside the contiguous United States.
- All Cloud-based applications and data storage must be FedRAMP capable.
- Data at rest and in transit must comply with FIPS 140-2 or most current standard.
- Data at rest and in transit from hosted or cloud-based applications must be compliant with all local, state, Federal and international regulations and guidelines appropriate to that data type.
- Cloud-based applications must have a multi-factor authentication feature that does not rely on security questions or email for the second verification.

- A third-party risk assessment, vulnerability scan, and penetration test must be issued for all new projects for which applications/solutions will be public-facing (on premises or cloud-based).

Application Standards:

- Applications that are not hosted are preferred to run on a virtual server in a VMware vSphere 6.5 environment and reside in the City's centralized data center.
- Application software must not require a user to be logged onto the desktop to run and operate. Application software must run as a service account, restricted from interactive log-in, or use similar technology.
- No hardware-based licensing keys are acceptable (examples: no dongles or USB licensing keys).
- Applications should be running with the lowest privileges possible. Applications requiring users to have local administrative rights for standard functions are not acceptable.
- The preferred client/server application development environment must meet our standards for supportability, compatibility and security.
- The preferred web-enabled development standards are MVC, CSS3, JavaScript, and HTML5; other application specific tools are also used.
- A web-based application must operate without browser or security (compatibility-mode) modifications.
- The preferred GIS standard is ESRI ArcGIS 10.7 or higher. Applications using map services are encouraged.
- The preferred version of Visual Studio is 2013 or higher.
- Applications and third-party plug-ins that are prerequisites for applications must be maintained to current supported versions.
- Alternative technical application environments may be proposed and will be considered on a case-by-case basis but are not guaranteed approval.
- The final configuration for all applications, including platform and development language, are subject to the approval of the Chief Information Officer or designee.

Database Standards:

- Preferred databases are Microsoft SQL Server 2016 Enterprise Edition in VMWare, or higher. SQL Server versions not supported by Microsoft or versions near end of support will not be permitted.
- Databases and SQL instances may reside and operate on a virtual server, reside and operate on a server shared with other SQL instances, or may require dedicated server hardware. Vendors must specify the minimum and preferred database hardware and software operating environment in their proposals.
- Alternative technical database environments may be proposed and will be considered on a case-by-case basis, but are not guaranteed approval.
- All datacenters for cloud-based or hosted applications and storage must reside within the contiguous United States. City of Norfolk data shall not be stored outside the contiguous United States.
- All City of Norfolk data used, input, updated or modified in the system is the sole property of the City of Norfolk and can be used by Norfolk staff or designated agents for any purpose.
- Data hosted in cloud services must be accessible by standard web protocols such as REST and SOAP APIs.
- The final configuration of all new servers and databases, including their physical and logical placement, are subject to the approval of the Chief Information Officer or designee.

Server Standards:

- The preferred web server standard is Microsoft Internet Information Server (IIS) and .NET, latest versions.
- The preferred server operating system is Windows Server 2016 or higher. Versions not supported by Microsoft or versions near end of support will not be permitted.
- The preferred server architecture is VMware. If there are technical reasons requiring dedicated servers, City of Norfolk Network/Database Administration staff can provide technical requirements.
- All servers must be running the RSA SecurID GINA and all personnel with Administrator rights must be issued an RSA hardware or software token. Alternate multi-factor authentication could be used if it is managed and controlled by City of Norfolk's Network/Security staff.
- All physical servers are preferred to reside in the City's centralized data center unless there are technical reasons requiring servers to be installed at other facilities. Alternative technical server environments may be proposed and will be considered on a case-by-case basis but are not guaranteed approval.
- The final configuration of all new servers and databases, including their physical and logical placement, are subject to the approval of the Chief Information Officer or designee.

Network Standards:

- Site to site Virtual Private Network (VPN) connections for cloud-based applications will be reviewed on a case-by-case basis.
- The network protocol is TCP/IP TLS 1.2 encryption protocol or higher.
- Select models of Cisco brand ISR routers, Catalyst model switches, and 2800/3800 model wireless access points are standard.
- Select models of Cisco voice and video network equipment are also standardized.
- The local network topology is 10/100/1000/10000 Mbps switched Ethernet, running on CAT6 twisted pair copper cabling, 50 UM multimode or single mode fiber optic cable. The wide area/metro network has multiple connection methods, including owned/leased MetroEthernet over HFC or fiber-optic, Fast Ethernet and Gigabit Ethernet services at various shaped bandwidths, and a 10Gbps DWDM-based Institutional Network (I-Net).

Network Communications Standards:

- All wired devices are located at facilities that are connected to the network on at least a cable modem using HFC/TLS services with minimum bandwidths of 1.5Mb upstream and 1.5Mb downstream and all are managed by the City. All others use a variety of communication bandwidths ranging from T-1 to OC-192 capacity.
- Wi-Fi wireless devices use the IEEE 802.11 b/g/n/ac standards.
- Broadband wireless devices use 4G Verizon Wireless CDMA standards. Unless specifically exempted by the City's technical staff, only imbedded 4G Verizon Wireless CDMA modems are permitted on mobile devices that will operate on the City's private Verizon Wireless provided mobile network.

Storage Standards:

- Centralized Storage Area Network (SAN) storage is available and preferred when appropriate. It consists of an 8Gbps Fiber Channel SAN attached to an Infinibox Storage Subsystem and used for all mission critical storage systems and VMware storage.

- There is a centralized enterprise class backup system which is located at the City's main data center. This backup system is Barracuda, which also provides redundant backup cloud storage.

Desktop/Laptop/Tablet Software Standards:

- Standard operating system is Windows 10 Professional (version 1903) x64 or higher.
- Currently devices running Apple MacOS , iOS, Linux, or any version of Android operating systems, are not allowed on the City's network, but are acceptable for off-network purposes with the approval of the Chief Information Officer or designee.
- Standard productivity suite is Microsoft Office 2016 Professional (Office 365) or higher. Other standard desktop software includes Nuance (latest version) for PDF reading/writing and WinZIP (latest version) for file compression.
- Standard and preferred web browser is Google Chrome or Microsoft Edge. Some versions of Internet Explorer are maintained for legacy application compatibility.
- Standard anti-virus software is the most current version of Symantec Endpoint Protection for devices running Microsoft operating systems and Sophos for devices running Apple Macintosh operating systems. All new application and database servers, workstations, laptops, tablets, etc. are required to operate with a copy of the appropriate anti-virus software.

Desktop/Laptop/Tablet Hardware Standards:

- Standard hardware for business desktops, laptops and tablets is the latest version of Dell Optiplex computers. There are two levels of models for desktops and laptops, one for general use and one for developer/performance use.
- There are various versions of ruggedized equipment in the environment, including Dell Optiplex, Getac, and Panasonic enterprise versions.

Cybersecurity Standards:

- The City currently uses Checkpoint NGTP appliances for intrusion protection, firewall, web filtering and other cybersecurity functions.
- Applications must be in-compliance with security patches no later than thirty days from the most recent vendor-released patches.
- Applications running Java must be in-compliance with security patches no later than ninety days from the most recent vendor-released patches.
- Web applications must be certified to work with high encryption for HTTPS traffic and support only TLS 1.2 encryption protocols. Group policies will be created to enforce this on servers and computers. Standalone systems, such as DMZ servers, will be performed manually.
- Any application to be installed must be listed in the agreement and must be vetted by Information Technology staff for licensing, security, and compatibility with other components on server or network.
- Vendors should not install backdoor or administrative accounts on the servers, applications or databases without providing all credentials to the City IT Security staff.
- No unchangeable hardcoded credentials shall be on applications. All credentials must be changeable by City staff at any time for any reason without negatively impacting application functionality.
- Vendors must safeguard the provided credentials to any City or external system configured for the City and must not share the credentials with anyone else. Should vendor suspect the credentials are compromised,

it must communicate this immediately to the City's point of contact.

- If vendor remote access to the application or server is required, it must be conducted via the most current version of Webex and should be recorded, both for training purposes and for forensics if needed. No Virtual Private Network (VPN) or RemoteApp access will be granted to non-City staff, regardless of location. A City staff member must be on the same conference call or access method and must be actively monitoring the work.
- Creation of Cloud services without IT involvement and approval in advance is discouraged and may not be supported. City of Norfolk staff have the right to disable or remove access to such services due to security concerns or compliance regulation violations.
- All datacenters for cloud-based or hosted applications and storage must reside within the contiguous United States. City of Norfolk data shall not be stored outside the contiguous United States.
- All Cloud-based applications and data storage must be FedRAMP capable.
- Data at rest and in transit must comply with FIPS 140-2 or most current standard.
- Data at rest and in transit from hosted or cloud-based applications must be compliant with all local, state, Federal and international regulations and guidelines appropriate to that data type.
- Cloud-based applications must have a multi-factor authentication feature that does not rely on security questions or email for the second verification.
- A third-party risk assessment, vulnerability scan, and penetration test must be issued for all new projects for which applications/solutions will be public-facing (on premises or cloud-based).