City of Andrews
Administrative Directive

Title: **Wireless Access Policy**		
Category: Finance		
Reference Number: Fin 3	Initial Effective Date: 4/1/2023	Last Revision Date:

1) SCOPE

This administrative directive provides guidelines regarding wireless access to the City of Andrews network and transportable media.

2) SPECIFIC PROTOCOLS AND DEVICES

2.1 WIRELESS USAGE STANDARDS AND POLICY

Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for City employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of City laptops and mobile devices.

Approval Procedure **-** In order to be granted the ability to utilize the wireless network interface on your City laptop or mobile device you will be required to gain the approval of your department director. The Network Access Request Form (found in Appendix A) is used to make such a request. Once this form is completed and approved you will be contacted by appropriate City personnel to setup your laptop and schedule training.

Software Requirements **-** The following is a list of minimum software requirements for any City laptop that is granted the privilege to use wireless access:

- Windows 10 with Service Pack 3 (Firewall enabled)
- Antivirus software
- Full Disk Encryption
- Appropriate VPN Client, if applicable
- Internet Explorer 6.0 SP2 or Greater

If your laptop does not have all of these software components, please notify your department director so these components can be installed.

Training Requirements **-** Once you have gained approval for wireless access on your City computer, you will be required to attend a usage and security training session to be provided by the Director of Finance or appropriate personnel. This training session

will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted.

2.2 USE OF TRANSPORTABLE MEDIA

Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the City in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from City networks. Every workstation or server that has been used by either City employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore, procedures must be carefully followed when copying data to or from transportable media to protect sensitive City data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a City employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is common within the City. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of City networks. Transportable media received from an external source could potentially pose a threat to City networks. ***Sensitive data*** includes all human resource data, financial data, City proprietary information, and personal information ("PI").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much-improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store City data or sensitive data must be an encrypted USB key issued by the Director of Finance. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the City.
- Non-City workstations and laptops may not have the same security protection standards required by the City, and accordingly virus patterns could potentially be transferred from the non-City device to the media and then back to the City workstation.

  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

- Data may be exchanged between City workstations/networks and workstations used within the City. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:
  Data provided to auditors via USB key during the course of the audit.

- It is permissible to connect transferable media from other businesses or individuals into City workstations or servers as long as the source of the media in on the City Approved Vendor list (Appendix D).
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Director of Finance or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves the City, all transportable media in their possession must be returned to the Director of Finance or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

The City utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Finance Director or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all City laptops, workstation, or servers must be wiped of data in a manner which conforms to regulations. All transportable media must be wiped according to the same standards. All transportable media must be returned to the Director of Finance or appropriate personnel for data erasure when no longer in use.

Appendix A – Network Access Request Form

Employee or Contractor Request for Network Access

EMPLOYEE/CONTRACTOR INFORMATION		
☐ New Employee ☐ New Contractor ☐ Existing User ☐ Temporary		Today's Date:
First Name:	Last Name:	*MI:
Position:	Department: Supervisor:	
☐ Full-time ☐ Part-time	Start date or Requested due date: Temporary or Contractor end date, if known:	

SECURITY

☐ Permit access to the following network location(s):

Drive	Path	Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
Drive	Path	Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access
Drive	Path	Access: ☐ Read-only ☐ Read/write ☐ Full Access ☐ Remove Access

☐ Miscellaneous Needs *(Enter any other requests)*:

DEVICE TO BE CONNTECTED TO NETWORK

Hardware:

☐ Laptop ☐ Desktop ☐ Either Laptop or Desktop
- ☐ Multifunction printer ☐ Netgear Router
- ☐ Standard inkjet printer ☐ Docking station

☐ iPhone ☐ iPad ☐ Windows Mobile Device

☐ Miscellaneous Needs *(Enter any other devices)*:

BUILDING ACCESS

Access Requested for the following location(s):

☐ Secure Storage ☐ Server Room
☐ Lobby ☐ Other, *Specify:*

Additional Access Restriction:

☐ After-Hours Access, *Specify Hours:*

Other Restrictions (be specific):

SPECIAL INSTRUCTIONS

Manager Checklist/Reminder:

- Signature below can be of the Department Director or the Data Owner if new network access is requested.
- Schedule new employee orientation, if applicable
- Ensure name appears on any appropriate sign-in/out sheets
- Remember to have all new employees/contractors read and sign appropriate forms, i.e., Confidentiality Form (Appendix B)
- Request appropriate training/background:
  - Security Training
  - Any additional training and/or background check

NAME	**SIGNATURE**	**DATE**
Department Director (Print Name)		
Director of Finance / Appropriate Authority		