Frequently Asked Questions (FAQ)

FAQ Table of Contents

City Systems

What major City systems may be accessed remotely—without using VPN?

- Access Irvine
- Access Irvine Admin Console
- Bonfire (RFP)
- Brainstorm (Application Training)
- CivicRec
- ClientTrack
- **eGovStrategies (Payment Processing)**
  - eGov Invoice Search
  - eGov Login
  - eGov Admin
  - eGov Permits Billing Lookup
- Employee Online (EOL)
- EPR (Plan Review)
- External GIS services
- Exigis
- GoPost
- Granicus Media Portal
- ICMA-RC (Deferred Compensation)
- IrvineQuickRecords
- Lucity Mobile
- Meetings & Agendas
- NeoGov
- **OnBase (*Public Safety*):**
  - Police Records Request
- Permits
- Public Records Request
- Raiser's Edge (Donations)
- Sire (Invoice Workflow)
- SANS (Cybersecurity Awareness Training)
- Trakstar (Evaluations)
- UGovernIT (Help Desk)
- Volgistics Volunteer
- Volunteer (1 Million-hour Challenge)
- VTI / IntelliTime (Timesheet)
- Work Load Management (Community Development)
- Workterra (Benefits)
- Workterra (Flexible Spending Account)

What major City systems are only accessible using the City network or via VPN?

- Eden (Permits)
- Lucity (Work Order Management)
- ONESolution (Finance/Enterprise Resource Planning)
- Shared drives (N: Drive, R: Drive)

- Intranet (insideirvine)

General Topics

What resources are available to staff to work remotely?

Email is available online and can be accessed remotely by visiting Microsoft Office 365 at www.office.com. The City supports remote work by providing a number of resources such as City-issued devices (laptops, mobile phones) and software that facilitates remote access. Users can also access their voice mail and email remotely. Many City applications are available via the internet (see City Systems section for examples).

How do I access my desktop remotely?

A Remote Desktop Connection to your City desktop will allow you to access your City desktop using Virtual Private Network (VPN) software. GlobalProtect is the primary VPN software the City uses. A director-level approval is required for VPN access. Please contact your IT Liaison to request access.

How do I secure my remote access?

The City currently uses Microsoft's Authentication application to secure user access. Helpdesk will contact active users to schedule the software installation and training in the coming weeks.

What are the major applications available in Microsoft Office 365?

Microsoft Office 365 is a cloud-based service that brings together a variety of tools.

- Outlook (email, contacts, calendar, tasks)
- Word
- Excel
- OneNote
- Forms
- SharePoint
- OneDrive

Who are the IT Liaisons?

- City Clerk/Records: Debbie Tracy & Taryn Tang
- City Manager's Office: Nicolle Rogers & Melissa Haley
- Community Development: Amy Roblyer
- Community Services: Jenn Starnes & Steven Stewart
- Financial Management and Strategic Planning: Kevin Saycocie, Brian Brown & Angie Burgh
- Human Resources & Innovation: Darrell Cheam & Chi Nguyen
- Public Safety: Jade Mazzio & Nick Rycroft
- Public Works and Transportation: Anna Sanchez & Tiffany Woods

Virtual Private Network (VPN) Access

In order to use the City's VPN to access your City desktop, you first must install Microsoft Authenticator and GlobalProtect software.

How do I install Microsoft Authenticator?

Click this link from the City network and follow the instructions: Installation Instructions for Microsoft Authenticator app. To access these instructions outside of the City network you may submit a Help Desk request.

How do I install GlobalProtect VPN software?

Click this link from the City network and follow the instructions: Installation Instructions for GlobalProtect VPN software. To access these instructions outside of the City network you may submit a Help Desk request.

Note: These instructions are also posted on the City's Intranet in the Technology Corner section.

How do I use Remote Desktop Connection?

After connecting to the City network, you may use Remote Desktop Connection to connect to a computer running Windows—from another computer running Windows. You will be able to use all of your City desktop computer's programs, files, and network resources from your approved remote device (desktops and laptops), as if you were sitting in front of your computer at work.

To remotely connect to your City desktop, the City desktop computer must be turned on, it must have a network connection, Remote Desktop must be enabled, you must have network access to the remote computer (this could be through the Internet), and you must have prior approved permission to connect via GlobalProtect VPN.

Before you start a connection, it is a good idea to look up the name of the computer you are connecting to. Click the 

icon on your desktop to display your computer name. Contact Help Desk if you have trouble finding the name of the desktop you would like to connect to. To connect:

1. Type **Remote Desktop Connection** in your Windows search box, and in the list of results click **Remote Desktop Connection**.
2. In the **Computer** box, type the name of the computer that you want to connect to, and then click the **Connect** button.

Online Meeting and Collaboration Tool

Does the City support an online meeting tool?

Yes. The City currently supports and has a limited number of Cisco WebEx accounts for use by City employees. To access the tool, please request director approval and submit a Help Desk request.

Laptops and Mobile Devices

Only City-issued laptops and mobile devices with up-to-date patches may be used to access secured City systems with sensitive or confidential information (e.g., Human Resources data with names, addresses, and Social Security numbers). For accessing email over the public internet, you may use a personal device such as a laptop, tablet, or mobile phone.

What is required to use my personal desktop/laptop to access City systems?

You may use your personal devices to connect to the City's Office 365 web-based subscription service to Microsoft Office suite of products (e.g., Outlook, Word, Excel, PowerPoint) as long as the device operating system is up-to-date with patches and if the device uses a virus protection program. To access Office 365, visit this website: https://www.office.com/ and enter your City log-on credentials.

Guidelines for Securing Personal Devices:

Unsecured Public Wi-Fi Networks. Do not connect to City information and network on unsecured Wi-Fi networks. Unsecured public Wi-Fi networks are prime spots for malicious parties to spy on internet traffic and lead to leakage of sensitive information.

Antivirus Software. A good antivirus software can act as the next line of defense by detecting and blocking known malware. Even if malware does manage to find its way onto your device, an antivirus may be able to detect and in some cases remove it. Norton, McAfee, and Bitdefender are some recommended options if you do not already have antivirus software.

Use strong passwords. It is as important as ever to ensure that all accounts are protected with strong passwords. Unfortunately, many people still use the same password across multiple accounts. This means that all it takes is one compromised password for a criminal to take over all of your accounts.

Set up two-factor authentication. Having a strong password often is not enough if your credentials are leaked in a data breach. Two -factor authentication (2FA) and two-step verification (2SV) involve an additional step to add an extra layer of protection to your accounts. The extra step could be an email or text message confirmation, a biometric method such as facial recognition or a fingerprint scan, or something physical, such as a USB fob.

Install security updates regularly. Updates to device software and other applications can be a source of annoyance. But they really are important. Updates often include patches for security vulnerabilities that have been uncovered since the last iteration of the software was released. In many cases, you can set updates to run automatically, often while you are sleeping, so you don't have to worry about downtime.

Look out for phishing emails and sites. Phishing emails, as well as voicemails (vishing) and text messages (SMS phishing or smishing) are used by cybercriminals to "phish" for information. This information is usually used in further schemes such as spear phishing campaigns (targeted phishing attacks), credit card fraud, and account takeover fraud.

With the rise in the number of people working from home, it is highly likely that phishing emails will target remote workers in a bid to steal their personal information or gain access to company accounts.

Watch out for work-from-home scams. As well as targeted phishing attacks, we're likely to see an increase in work-from-home scams and other schemes that typically target gig economy workers. Many of these request personal information or upfront payments before you can begin work. By the time you realize it is a scam, the fraudster has ceased contact and stolen your money or taken over accounts.

Lock your device. If you do have to work in a public space, or if you live with people who you can't share work information with, then it is important to keep your device secure. Password-locking your device will usually encrypt its contents until someone enters the password.

What is required to take City equipment home for work use (Monitors and Accessories)?

Director approval is required to take non-mobile equipment such as monitors and accessories for work-from-home use.

City Desk Phones

How may I setup a conference call using my City desk phone?

To forward all calls:

1. From an active call, press the **Conference**  button.
2. Enter the phone number for the party you want to add to the conference and press **Dial.**
3. Repeat the above for up to six total callers (including your phone).
4. Press the **Conference** soft key.
5. The conference is active.

May I forward my desktop phone line to my personal or City-issued mobile phone?

No. Users are not allowed to forward City desktop phone lines to mobile phones.

How may I access my voice messages from a personal phone?

Users may listen to their voice messages by dialing 949-724-5403 and providing the phone extension and Personal Identification Number (PIN).

How may I access my email messages from a personal phone?

Users may listen to their email, narrated by the phone system, by dialing 949-724-5403 and providing the phone extension and PIN. Select Option #2 to listen to email messages.

What methods exist to block the display of personal phone numbers?

To be 100% sure of protecting your personal information you should contact your personal carrier and/or the manufacturer of your mobile device to ensure that your number is properly blocked as carrier processes may be different and subject to change, however, here are some generally known guidelines:

- Verizon, T-Mobile, Sprint (Enter *67, Enter the number you want to call then initiate the call. Do this for each call.). Example: *67 555-555-1234
- Bell (#31# before each number called)
- To permanently block your number from appearing on outgoing calls, you would have to contact your carrier. To have the number display in this blocked configuration, enter *82 to unblock single calls.
- Android device (Settings > Click Call settings > Click Additional Settings > Click on Caller ID > Choose "**Hide number**" and your number will be hidden. Choose "**Show number**" to resume showing your number.

We strongly suggest that you test each process before making calls where you wish to prevent personal information displaying.

Support

How do I get support for questions not included in the FAQ?

Contact the City of Irvine Help Desk:

- Call: 949-724-HELP (949-724-4357)
- eMail: helpdesk@cityofirvine.org
- Self-Service Ticket: Visit Technology Corner on the Intranet - http://intranet/departments/information_technology/service_catalog.asp
- UGovernIT (Help Desk ticket system available via the internet) - https://cityofirvine.ugovernit.com/