

Networking Checklist

Whether you are an office of one or 100, it's easy to network Drake Software with a dedicated server or peer-to-peer network. This list is intended for use by the office IT Technician to ensure that the office networking needs are met prior to the start of a new tax season. Keep this checklist for your records. Drake Software can be networked using either the preferred method Server-Only (NW Client) or Alternative Server Configuration method.

Part 1 - Network Setup

Step 1

(If installing Drake Software as a separate installation on every workstation, Skip to Step 2.)

Dedicated Server Configuration (Preferred Network Installation)

- Does the office have a Server-Only (NW Client)? __Y __N
- If so, is there sufficient memory and hard drive capacity to operate efficiently? __ Y __N
- Have new machines been added to the network? __ Y __N
- If so, is NW Client installed on each machine? __ Y __N
- Does the operating system need to be upgraded? __ Y __N
- Are the Directories and Paths set properly on the server and workstations? __ Y __N
- Is there an NW Client link on each workstation mapped to the server? __ Y __N
- Is the drive mapped correctly? __ Y __N
- What is the drive letter? _____

Step 2

- Alternate Server Configuration (Drake installed on all computers)
- Does the office have an Alternate Server Configuration? __Y __N
- If so, is there sufficient memory and hard drive capacity to operate efficiently? __ Y __N
- Have new machines been added to the network? __ Y __N
- Does the operating system need to be upgraded? __ Y __N
- Are the Directories and Paths set properly on the server workstation and workstations? __ Y __N
- Is the drive mapped correctly? __ Y __N
- What is the server drive letter? _____

Part 2 - Drake Software Installation

- Is the software installed to the Root Directory on each machine or server? __ Y __N
 - Is it loaded on each machine if the office has a Multiple Computer Installation? __ Y __N
 - Are the permissions and sharing configured correctly on the server? __ Y __N
 - Is the software mapped correctly from the workstation to the server or workstation? __ Y __N
-

Networking Checklist

Part 3 - Evaluate the Office Computers

- Do you need to upgrade the memory? __ Y __ N
- Do you need to upgrade to a new operating system for increased performance? __ Y __ N
- Does the office need additional machines? __ Y __ N Have they been ordered? __ Y __ N
- Is there backup media for each machine? __ Y __ N
- If you are considering system upgrades or purchasing a new machine see Recommended System Requirements (if upgrading or purchasing a new computer)

Part 4 - System Requirements

Does the office meet the following recommended minimum system requirements?

- 1 GHz processor
- 1 GB of RAM for 32-bit and 2 GB of RAM for 64-bit
- Monitor capable of 1024 x 768 screen resolution
- CD drive (unless choosing download option)
- 1 GB of available hard drive space
- HP-compatible laser printer
- Internet Explorer 11
- Internet access (required for regular updates and PPR software)
- These are the minimum requirements to run Drake Software on most systems. For superior performance, we recommend system upgrades above the stated minimums. Actual requirements will vary based on your system configuration and the features and other programs you wish to install.

Printers

- Are they networked correctly? __ Y __ N
- Are printer's HP-compatible laser printer with support for the PCL-5e printer language and the Arial font? __ Y __ N
- If not, what types of printers are installed? _____

Cables

- Are there networking cables for each machine? __ Y __ N
- Are there proper cables for Internet connections? __ Y __ N

Internet

- Does the office have a high-speed internet connection? __ Y __ N
 - Is it available 24/7 for auto-install of updates? __ Y __ N
-

Networking Checklist

Antivirus / Firewall Configuration

- Is there a Firewall? __ Y __N
- What type is it? _____
- Is it configured to allow Drake Software to get updates and transmit files? __ Y __N
- Is there Antivirus Software? __ Y __N
- What type is it? __ Y __N
- Is it configured to not scan the Drake Software Folders? __ Y __N

Multi-Office

- Are there connections to each office? __ Y __N
- Is Drake Software installed correctly? __ Y __N
- Are permissions and sharing configured correctly if the offices are sharing files? __ Y __N
- Is the Multi-Office Manager (MOM) configured properly? __ Y __N
- Are the firewalls set to allow transmissions through? __ Y __N

Recommended System Requirements (if upgrading or purchasing a new computer)

- Windows 7, 8 or 10 Professional 64-bit
 - 2.8 GHz processor
 - 4 GB RAM
 - Monitor capable of 1280 x 1024 screen resolution
 - High-speed internet access (recommended for GruntWorx, SecureFilePro, Google and Outlook Calendar integration)
 - TWAIN-compliant scanner (recommended for Drake Documents)
-



Protect Your Clients. Protect Yourself.

Tax professionals must remember that they have a legal requirement under federal law to protect taxpayer information.

Monitor for Fraud

- Watch for returns and acknowledgements for taxpayers who you do not know or who you have not filed for yet.
- e-Services offers tools to help safeguard you and your clients.
 - Monitor and compare the number of returns being filed with your EFIN.
 - Utilize e-Services for ID Theft to get an IP PIN.

If you notice anything suspicious, contact Drake Compliance at 866.273.9032.

User Accounts

- Do not let an IT person set up your account...DO IT YOURSELF!
- Owner of the Drake Account/Software should be the Admin and know all passwords and security questions.
- Do not give Admin access to other employees or you could lose control over your account.
- Make sure Security Questions are answered truthfully with real answers otherwise you could forget them. Do not use the same answer for each or make up an answer.

Email accounts

An email account is the gateway into your life which, unfortunately, means it's also a valuable target for hackers and cyber criminals. The common email inbox can be exploited to leave all of your sensitive data open to compromise. Perhaps it's unsurprising that attacks on email accounts are common.

- Protect your email accounts by not allowing others access.
- Use strong passwords.
- Change your password on a regular basis.
- Take advantage of two-factor authentication.

Passwords

Drake Software complies with IRS requirements for passwords.

- Creating your password **DO'S...**
 - At least 8 characters (longer is better)
 - Use passphrases instead of passwords
 - Construct your password using a combination of lowercase and uppercase letters, numbers and special characters
- Creating your password **DON'TS...**
 - Start with uppercase letters
 - Use keyboard sequence (qwerty)
 - Use names of family members or friends, pet names, dates, phone numbers, etc.
 - Use dates that are significant to you.
- Protecting Your Password – **DON'TS**
 - Give your password to anyone
 - Write your password down
 - Use the same password for multiple systems sites
 - Rotate 3 or 4 passwords



Phishing Scams

Phishing is an email scam that attempts to obtain sensitive information, such as usernames, passwords, and credit card details, often for malicious reasons.

- Don't click on attachments unless they are expected and come from a known and trusted source.
- Hover your mouse over the links in each email message to display the actual URL. Check whether the hover-text link matches what's in the text, and whether the link looks like a site with which you would normally do business.
- Don't believe everything you see. Just because an email has convincing brand logos, language, and a seemingly valid email address, does not mean that it's legitimate.
- Be skeptical when it comes to your email messages—if it looks even remotely suspicious, don't open it.
- Use security software to help defend against malware, viruses, and known phishing sites and update the software automatically.

VPN/Remote Access

Many popular, highly-rated VPN services will leak your IP address, infect your computer with malware, install hidden tracking on your devices, steal your private information, leave your data exposed to hackers and mass surveillance, and even steal your bandwidth.

- If you must have remote access be sure to close it before leaving at the end of every day. Leaving access open can leave your entire network vulnerable.
- Free versions of VPN software typically do not have the security features of a good quality service so choose wisely.

e-Services and EFIN Documentation

- IRS requires that all Tax Software Providers have proper EFIN documentation on file.
 - The e-File Application Summary is the only document the IRS has designated as valid for EFIN registration.



Protect Your Clients; Protect Yourself

It takes all of us working together to protect taxpayers' data. The Data Security Resource Guide for Tax Professionals can help. Download it today at [IRS.gov/ProtectYourClients](https://www.irs.gov/ProtectYourClients).



Data Security Tips for Tax Professionals

Go to www.irs.gov/ProtectYourClients to download the complete Data Security Resource Guide for Tax Professionals. See what steps you can take to better protect your clients and your business.

Here's a sampling from the Data Security Resource Guide:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, e-Services, a tax software provider or cloud storage provider. Never open a link or any attachment from a suspicious email. Remember: The IRS never initiates initial email contact with tax pros about returns, refunds or requests for sensitive financial or password information.
- Create a data security plan using IRS [Publication 4557](#), Safeguarding Taxpayer Data, and [Small Business Information Security – The Fundamentals](#), by the National Institute of Standards and Technology.
- Review internal controls:
 - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets and phones) and keep software set to automatically update.
 - Use strong and unique passwords of 8 or more mixed characters, password protect all wireless devices, use a phrase or words that are easily remembered and change passwords periodically.
 - Encrypt all sensitive files/emails and use strong password protections.
 - Back up sensitive data to a safe and secure external source not connected fulltime to a network.
 - Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
 - Limit access to taxpayer data to individuals who need to know.
 - Check IRS e-Services account weekly for number of returns filed with EFIN.
- Report any data theft or data loss to the appropriate [IRS Stakeholder Liaison](#).
- Stay connected to the IRS through subscriptions to [e-News for Tax Professionals](#), [QuickAlerts](#) and [Social Media](#).

The Data Security Resource Guide for Tax Professionals also details the signs of data thefts, explains how to report thefts to IRS and provides links to important data theft resources on IRS.gov. Download your guide today.





Proteja a sus clientes; Protéjase a sí mismo

Para proteger los datos de los contribuyentes, todos tenemos que trabajar juntos. La *Guía de Recursos de Seguridad de Datos para los Profesionales de Impuestos* le puede ayudar. Descárguela hoy en [IRS.gov/ProtectYourClients](https://www.irs.gov/ProtectYourClients).



Consejos sobre la Seguridad de Datos para los Profesionales de Impuestos

Visite www.irs.gov/ProtectYourClients, para descargar completa la Guía de Recursos de Seguridad de Datos para los Profesionales de Impuestos. Vea los pasos que puede tomar para proteger mejor a sus clientes y a su negocio.

A continuación, una muestra de la Guía de Recursos de Seguridad de Datos:

- Aprenda a reconocer los correos electrónicos de *phishing*, sobre todo aquellos que fingen ser del IRS, de servicios electrónicos, un proveedor de software tributario o un proveedor de almacenamiento en la nube. Nunca pulse en un enlace ni abra cualquier anexo de un correo electrónico sospechoso. Recuerde: El IRS nunca inicia contacto inicial por correo electrónico con los profesionales de impuestos sobre las declaraciones, reembolsos o solicitudes de información financiera o de contraseñas confidenciales.
- Establezca un plan de seguridad de datos, utilizando la [Publicación 4557](#) del IRS, *Safeguarding Taxpayer Data* (Cómo salvaguardar los datos del contribuyente), en inglés, y [Small Business Information Security – The Fundamentals](#) (Seguridad de la Información de Negocios Pequeños – Los Fundamentos), en inglés, del Instituto Nacional de Estándares y Tecnología.
- Revise los controles internos:
 - Instale el software de seguridad *anti-malware/anti-virus* en todos los dispositivos (computadoras portátiles, computadoras de escritorios, enrutadores, tabletas y teléfonos) y mantenga el software configurado para que se actualice automáticamente.
 - Utilice contraseñas fuertes y únicas de 8 o más caracteres mixtos, las contraseñas protegen todos los dispositivos inalámbricos; utilice una frase o palabras que sean fáciles de recordar y cambie las contraseñas periódicamente.
 - Encripte todos los archivos/correos electrónicos y utilice contraseñas fuertes para protegerlos.
 - Haga una copia de seguridad de sus datos confidenciales y guárdela en un lugar externo y seguro que no esté conectado a tiempo completo a una red.
 - Borre o destruya los discos duros de las computadoras e impresoras anteriores que contengan datos confidenciales.
 - Limite el acceso a los datos de los contribuyentes a sólo a las personas que tienen que saberlos.
 - Verifique semanalmente la cuenta de los servicios electrónicos del IRS, para ver el número de declaraciones presentadas con el Número de Identificación de Presentación Electrónica (*EFIN*, por sus siglas en inglés).
- Informe todo robo o pérdida de datos al [Enlace del IRS con las partes interesadas](#) (en inglés) apropiado.
- Manténgase conectado con el IRS a través de las inscripciones al [Boletín electrónico](#) para los [Profesionales de Impuestos](#) (en inglés), [QuickAlerts](#) (en inglés) y los [Medios Sociales](#).

la Guía de Recursos de Seguridad de Datos para los Profesionales de Impuestos también detalla las señales de robos de datos, explica cómo informar de robos al IRS y proporciona enlaces a recursos importantes sobre el robo de datos en [IRS.gov](https://www.irs.gov). Descargue su guía hoy.

