This document is a Work-In-Progress and may contain errors, typo's, etc.. Please email shaun@copscorp.com.au with any corrections or to request any additions or changes

Cheat Sheet

Apps

Windows

App	Install	Description	Use Case
AMD Adrenalin			
Apple iTunes	`winget install Apple.iTunes`		DEPRECATE-DUse `Apple Devices` instead
Apple Devices	`winget install "Apple Devices"`		
Clear Disk Info	`winget install Carifred.ClearDiskInfo`		
CPUID CPU-Z	`winget install CPUID.CPU-Z`		
CPUID HWMonitor	`winget install CPUID.HWMonitor`		
CrystalDiskInfo	`winget install CrystalDewWorld.CrystalDiskInfo`		DEPRACATED-Misreports SMART data on some drives, use `Clear Disk Info` instead
CrystalDiskMark	`winget install CrystalDewWorld.CrystalDiskMark`		
Display Driver Uninstaller (DDU)	`winget install Wagnardsoft.DisplayDriverUninstaller`		
FileZilla			

App	Install	Description	Use Case
ForensiT Transwiz	`winget install ForensiT.Transwiz`		DEPRECATED-Breaks with newer OneDrive and Windows 11 releases, manually copy %USERPROFILE% instead
Furmark	`winget install Geeks3D.FurMark.2`		
GPU-Z	`winget install TechPowerUp.GPU-Z`		
Intel HD Graphics			
Libre Office	`winget install TheDocumentFoundation.LibreOffice`		
Microsoft Office	`winget install Microsoft.Office`		
Microsoft PC Health Check	`winget install Microsoft.WindowsPCHealthCheck`		
Microsoft Visual Studio Code	`winget install Microsoft.VisualStudioCode`		
Microsoft Windows Terminal	`winget install Microsoft.WindowsTerminal`		
Microsoft Verifier			
MiniTool Partition Wizard	`winget install MiniTool.PartitionWizard.Free`		
NirSoft BlueScreenView	`winget install NirSoft.BlueScreenView`		
NirSoft Product Key Scanner			
NirSoft ProduKey			
Nvidia App			
RevoUninstaller	`winget install RevoUninstaller.RevoUninstaller`		
Snappy Driver Installer Origin (SDIO)	`winget install GlennDelahoy.SnappyDriverInstallerOrigin`		
Sublime Text	`winget install SublimeHQ.SublimeText.4`		

App	Install	Description	Use Case
TeamViewer	`winget install TeamViewer.TeamViewer`		
UltraViewer	`winget install DucFabulous.UltraViewer`		
Ultra Virus Killer (UVK)			
Google Chrome	`winget install Google.Chrome`		
Mozilla Firefox	`winget install Mozilla.Firefox`		
Mozilla Thunderbird	`winget install Mozilla.Thunderbird`		
eM Client	`winget install eMClient.eMClient`		
Disk Drill	`winget install CleverFiles.DiskDrill`		
HWiNFO	`winget install REALiX.HWiNFO`		
Cinebench	`winget install Maxon.CinebenchR23`		
VLC	`winget install VideoLAN.VLC`		
GitHub Desktop	`winget install GitHub.GitHubDesktop`		
Trend Micro Internet Security	`winget install "Trend Micro Internet Security"`		
Trend Micro Maximum Security	`winget install "Trend Micro Maximum Security"`		
HashCheck Shell Extension	`winget install idrassi.HashCheckShellExtension`		
Git	`winget install Git.Git`		
MakeMKV	`winget install GuinpinSoft.MakeMKV`		
HD Tune Pro	`winget install EFDSoftware.HDTunePro`	HDD / SSD Utility	Benchmark drive speed over time with graph
7-Zip			
AltSnap			
BandiZip			

App	Install	Description	Use Case
BandiView			
Bitwarden			
Winget			
Chocolatey			
FFmpeg			
FileBot			
HandBrake			
iPerf			
JDownloader			
HexChat			
qBittorrent			
MediaInfo			
Microsoft			
OneDrive			
Google Drive			
DropBox			
NVIDIA GeForce Experience			DEPRECATE-DUse `NVIDIA App` instead
Papa's Best STL Viewer			
PowerToys			
Proton VPN			
ReNamer			
Rufus			
BalenaEtcher			
SD Card Formatter			
Raspberry Pi Imager			
WinRAR			
Win32 Disk Imager			
WizTree			
Everything			
yt-dlp	`winget install yt-dlp.yt-dlp`		
Audacity			
Exact Audio Copy (EAC)			
OpenOffice			
Inkscape	`winget install Inkscape.Inkscape`		

macOS

App	Install	Description	Use Case
Apple Image Capture		Download photos/videos from digital cameras or iOS devices	Useful for backing up photos/videos from iOS devices, even if their iCloud account isn't working, as it treats the iOS device like a digital camera and simply imports the local copies on the device

iOS

Android

App	Description	Use Case
Appwatch	Snitch on app activity	DEPRECATEDUse `Rox Security` instead
Aurora Store	Alternative `Google Play Store` app	Install apps from the Play Store repository without needing to log in with a Google Account, and can download .APKs from the Play Store for later sideloading
Rox Security	Multi-tool for identifying unusual/unwanted app behaviour, including snitching on app activity	Identify apps that are responsible for instrusive full-screen pop-ups

Commands

Windows

Command	Description	Use Case
`\`	Opens `%SYSTEMDRIVE%` folder	Quick access to `C:\`
`appwiz.cpl`	Opens `Programs and Features` control panel window	
`calc`	Opens `Calculator` app	
`charmap`	Opens `Character Map` app	
`chrome`	Opens `Google Chrome` app *(if installed)*	
`cmd`	Opens `Command Prompt` app *(if installed)*	
`code`	Opens `Visual Studio Code` app	
`compmgmt.msc`	Opens `Computer Management` snap in	
`control`	Opens `Control Panel`	
`control folders`	Opens `File Explorer Options` window	
`control keyboard`	Opens `Keyboard Properties` window	
`control printers`	Opens `Bluetooth & devices` settings window	Quick access to `Printers & scanners`
`control update`	Opens `Windows Update` settings window	
`desk.cpl`	Opens `Display` settings window	
`devmgmt.msc`	Opens `Device Manager` snap in	
`diskmgmt.msc`	Opens `Disk Management` snap in	
`diskpart`	Opens `Microsoft DiskPart` command line interface	
`documents`	Opens current user's `Documents` folder	
`downloads`	Opens current user's `Downloads` folder	
`dxdiag`	Opens `DirectX Diagnostic Tool` app	
`eventvwr.msc`	Opens `Event Viewer` snap in	

Command	Description	Use Case
`explorer`	Opens `Windows Explorer`	
`firefox`	Opens `Mozilla Firefox` app *(if installed)*	
`firewall.cpl`	Opens `Windows Defender Firewall` control panel window	
`fonts`	Opens `Fonts` folder	
`gpedit.msc`	Opens `Local Group Policy Editor` snap in	
`iexplore`	Opens `Internet Explorer` app	
`inetcpl.cpl`	Opens `Internet Properties` window	Quick access to `Proxy server` settings
`joy.cpl`	Opens `Game Controllers` window	Use to test game controller inputs
`lusrmgr.msc`	Opens `Local Users and Groups` snap in	Powerful control over User Accounts and Groups, but does not work on Windows Home editions
`main.cpl`	Opens `Mouse Properties` window	
`manage-bde c: -off`	Run in a terminal to decrypt and disable `BitLocker` on C: drive	
`manage-bde -status`	Run in a terminal to show `BitLocker` status of all drives	
`mdsched`	Opens `Windows Memory Diagnostic` app	
`mmc`	Opens empty `Microsoft Management Console` snap in	
`mmsys.cpl`	Opens `Sound` window	
`mrt`	Opens `Microsoft Windows Malicious Software Removal Tool` app	
`msconfig`	Opens `System Configuration` window	Quick access to `Safe boot` or Windows boot entries

Command	Description	Use Case
`msedge`	Opens `Microsoft Edge` app	
`msinfo32`	Opens `System Information`	
`mstsc`	Opens `Remote Desktop Connection` app	
`ms-windows-store:`	Opens `Microsoft Store` app	
`ncpa.cpl`	Opens `Network Connections` control panel window	
`netplwiz`	Opens `User Accounts` window	Less powerful control over User Accounts, but does work on Windows Home editions
`notepad`	Opens `Notepad` app	
`onedrive`	Opens current user's `OneDrive` folder	
`osk`	Opens `On-Screen Keyboard`	
`pictures`	Opens current user's `Pictures` folder	
`powercfg.cpl`	Opens `Power Options` control panel window	
`powershell`	Opens `Powershell` app	
`regedit`	Opens `Registry Editor` app	
`resmon`	Opens `Resource Monitor app`	
`services.msc`	Opens `Services` snap in	
`shell:appsfolder`	Opens `Applications` folder	Useful for creating shortcuts to `Microsoft Store` apps
`shell:mycomputerfolder`	Opens `This PC` folder	
`shell:recyclebinfolder`	Opens `Recycle Bin` folder	
`shell:startup`	Opens `Startup` folder	
`shutdown -h`	Hibernate computer	
`shutdown -l`	Log off	
`shutdown -r -fw`	Restart Windows and boot in to `BIOS` / `UEFI`	
`shutdown -r -o`	Restart Windows and boot in to `Recovery Environment`	

Command	Description	Use Case
`shutdown -r -f -t 00`	Force Restarts Windows immediately	
`shutdown -s -f -t 00`	Force Shuts down Windows immediately	
`snippingtool`	Opens `Snipping Tool` app	
`sysdm.cpl`	Opens `System Properties` window	Quick access to `System Restore`
`taskmgr`	Opens `Task Manager` app	
`taskschd.msc`	Opens `Task Scheduler` snap in	
`timedate.cpl`	Opens `Date and Time` window	
`verifier`	Opens `Driver Verifier Manager` app	
`videos`	Opens current user's `Videos` folder	
`vlc`	Opens `VLC Media Player` app *(if installed)*	
`winver`	Opens `About Windows` window	Quick way to check installed Windows edition *(Home/Pro/Enterprise)*, version, and build
`wt`	Opens `Windows Terminal` app	
`%APPDATA%`	Opens current user's `AppData\Roaming` folder	
`%LOCALAPPDATA%`	Opens current user's `AppData\Local` folder	
`%SYSTEMDRIVE%`	Opens the root folder of the system drive	
`%TEMP%`	Opens current user's `Temp` folder	
`%USERPROFILE%`	Opens current user's profile folder	
`%WINDIR%`	Opens `Windows` folder	

Hotkeys

Windows

Resources

Hardware

iFixIt Electronics Skills
iFixIt Repair Guides
Repair Wiki
Keyboard Checker

Networking

Port Forward
SpeedTest

Security

Bitwarden Password Generator
(Type = Passphrase, Capitalize = Y, Include Number = Y, Word Separator = -, Length = 3)
Have I Been Pwned

Phonetic Alphabet

The NATO Phonetic Alphabet can be very useful when trying to provide remote support over the phone

Letter	Word
A	Aplha
B	Bravo
C	Charlie
D	Delta
E	Echo
F	Foxtrot
G	Golf
H	Hotel
I	India
J	Juliett
K	Kilo
L	Lima
M	Mike
N	November
O	Oscar

Letter	Word
P	Papa
Q	Quebec
R	Romeo
S	Sierra
T	Tango
U	Uniform
V	Victor
W	Whiskey
X	X-ray
Y	Yankee
Z	Zulu

System Service

Windows

Software

- **Restart Windows**
  Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean environment befor proceeding
- **System Restore**
  Check System Restore configuration and try to set at least 7% allocation
- Create a new System Restore point
  Name it something like `COPS - Pre System Service`
- **Task Manager**
  - Disable unwanted startup items
- **Wintoys**
  - Install Wintoys
    `winget install wintoys`
    or
    `winget install 9P8LTPGCBZXD`
    or
    `ms-windows-store://pdp/?ProductId=9P8LTPGCBZXD`
  - Performance Tab
    - `Ultimate performance power plan`
      Turn ON if Desktop
      Turn OFF if Laptop
    - `HAGS (hardware-accelerated GPU scheduling)` | Turn ON
    - `VBS (virtualization-base security)` | Turn ON
    - `Startup apps` | Disable unwanted startup items

        - `Search indexing` | Turn ON
        - `Delivery optimization` | Turn ON
        - `Network adapter onboard processor` | Turn ON
    - Health Tab
        - `Fast startup` | Turn ON
        - `Drive optimization` | Turn ON and run (click config icon and optimise each drive)
        - `Storage sense` | Turn ON and run (click config icon and click 'Run Storage Sense now')
        - `Cleanup` | Run 'Junk' + 'Microsoft Store' + 'DNS'
        - `System updates` | Set to 'Default'
        - `App updates` | Turn ON
        - `Graphics driver` | Click 'Restart'
        - `Icons cache` | Click 'Rebuild'
    - Tweaks Tab
        - `Desktop` | Turn ON 'This PC' + 'Recycle Bin'
- Update software
    - Windows Update
        - *old Windows 10 builds can use the Windows 10 Update Assistant to jump to the latest build*
    - Update Apps via Winget
    - Update Apps via Microsoft Store
    - Update Office Apps
- Update Drivers
    - Update Drivers using `SDIO`
    - Verify Drivers using `verifier`
- Maintenance
    - Run the following commands:
        - sfc /scannow
        - dism /online /cleanup-image /startcomponentcleanup /resetbase
        - dism /online /cleanup-image /restorehealth
        - sfc /scannow
        - chkdsk c: /r /scan /perf
        - defrag c: /o
    - Disk Cleanup
        - Run `cleanmgr /sageset:10`
        - Click `Clean up system files`
        - Tick all checkboxes EXCEPT: `System error memory dump files` `System error minidump files` `Windows error reports and feedback diagnostics` `User file history`
        - Click `OK`
        - Run `cleanmgr /sagerun:10`
    - Memory Diagnostics
        - Run `Windows Memory Diagnostics`
        - Click 'Restart now and check for problems (recommended)'
        - After Windows boots back up, check results: `Event Viewer` -

Windows Logs - System - Filter Current Log... - Event sources - Tick 'MemoryDiagnostics-Results' - Click OK
- Create a new System Restore point*Name it something like "COPS - Post System Service"*

Hardware

- Check all buttons and ports are free from debris and working functioning correctly
- Air compress out system as required
- Wipe down device and clean surfaces
- Add a `Serviced by COPS` sticker or replace old worn stickers as required

Data Transfer

Windows

Backup

- **Restart Windows**
  Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean environment befor proceeding
- [OPTIONAL] Create a new System Restore point
- **Disable Antivirus**
  - *Some of our extraction tools prompt false positives in the majority of security software*
- **Create a Job folder on a Transfer Drive**
  naming convention:
  `Job#5000`
  - *Create a new folder with the current job number to save User Data to*
- **Backup User Profiles**
  - *Copy `C:\Users\` folder to the Job folder on the Transfer Drive*
- **Backup Web Browsers**
  For each web browser installed complete the following:
  - **Export Bookmarks**
    naming convention:
    `Web Browser - Google Chrome - Bookmarks - 2024-07-15.html`
    or
    `web-browser_google-chrome_bookmarks_2024-07-15.html`
    - *Google Chrome URL:* `chrome://bookmarks`

    - *Microsoft Edge URL:* `edge://favorites`
    - *AVG Secure Browser URL:* `secure://bookmarks`
    - *Mozilla Firefox Hotkey:* `Ctrl+Shift+O`
    - *Microsoft Internet Explorer:* `%USERPROFILE%\Favorites`
- **Export Passwords**
  naming convention:
  `Web Browser - Google Chrome - Passwords - 2024-07-15.csv`
  or
  `web-browser_google-chrome_passwords-2024-07-15.csv`
    - *Google Chrome URL:* `chrome://password-manager` or `chrome://settings/passwords` (older Chrome versions)
    - *Microsoft Edge URL:* `edge://wallet/passwords` or `edge://settings/passwords` (older Edge versions)
    - *AVG Secure Browser URL:* `secure://password-manager` or `secure://settings/passwords` (older Secure Browser versions)
    - *Mozilla Firefox URL:* `about:logins`
    - *Microsoft Internet Explorer:* use Nirsoft IE PassView
- **Sync Accounts**
  Try to sync each browser with their relevant accounts if available
  Manual exports of Bookmarks + Passwords is good, but syncing the entire browser is better
    - *Google Chrome:* `Google Account`
      - `chrome://sync-internals`
      - Check Enabled: `Sync Feature Enabled` = true
      - Check Account: `Username`
      - Checked Synced: `Last Synced` = Just now
      - Check Not Actively Syncing: `Sync Cycle Ongoing` = false
      - Force Sync (if required): `chrome://extensions` - enable `Developer mode` - click `Update`
    - *Microsoft Edge:* `Microsoft Account`
      - *TODO (but it's similar to Chrome)*
    - *AVG Secure Browser:* `AVG Account`

        - *TODO (but it's similar to Chrome)*

    - Mozilla Firefox:_ `Mozilla Account`
        - *TODO*
- **Export Installed Programs List**
  naming convention:
  `Installed Programs - Nirsoft Uninstallview - 2024-07-15.html`
  or
  `installed-programs_nirsoft-uninstallview_2024-07-15.html`
    - *use Nirsoft UninstallView, save all as Horizontal HTML*
- **Export Winget**
  naming convention:
  `Winget - Export - 2024-07-15.json`
  or
  `winget_export_2024-07-15.json`
    - Open a Terminal as Administrator
      Run `wt` or `powershell` or `cmd`
    - Check Winget is installed `winget -v` (this will throw an error if winget is unavailable)
    - Update Winget `winget source update`
    - Export Winget's list of installed programs `winget export -o "REPLACE-WITH-TARGET-FILE"`
      (update REPLACE-WITH-TARGET-FILE with the target winget export file on the transfer drive)
    - Optionally export a list of all programs that Winget does cannot re-install at the same time with this extended command `winget export -o "REPLACE-WITH-TARGET-FILE" >- "winget_unnavailable.txt"`
- **Export License Keys**
  naming convention:
  `License Keys - Nirsoft Product Key Scanner - 2024-07-15.html`
  or
  `license-keys_nirsoft-product-key-scanner_2024-07-15.html`
    - *use Nirsoft Product Key Scanner or Nirsoft ProduKey, save all as Horizontal HTML*
- **Export Emails**
    - Extract Passwords and Server Settings
        - Nirsoft Mail PassView
        - Nirsoft WinMailPassRec
        - Nirsoft PstPassword
    - Backup any accounts set up as POP
        - *How to export emails to file in Outlook*
- **Check C: Drive for unusual files/folders**
    - *copy to Job folder copying the C: Drive file structure (Transfer-*

Drive:\Job#5000\C\FolderToSave)

- [OPTIONAL] Create Winget Install Script
  - *https://winstall.app/ - Select Desired Programs - Generate Script - Download both Batch (.bat) and PowerShell (.ps1) scripts*
- **Export Drivers**
  `TRANSFERDRIVE:\\Job#5000\Drivers - 2024-07-15\`
  or
  `TRANSFERDRIVER:\\Job#5000\drivers_2024-07-15\`
  - *Open* `PowerShell` *as an Administrator and run the following script:* `Export-WindowsDriver -Online -Destination "REPLACE-WITH-TARGET-FOLDER"`
    (update REPLACE-WITH-TARGET-FOLDER with the target drivers folder on the transfer drive)
- **Enable Antivirus**

Prepare New Device *(if required)*

- **Create a Local Account during Windows 10/11 Out of Box Experience (OOBE)**
  - **Option 1: No Internet Connected**
    Bypass Network Registration
    - *Open Command Prompt:* `Shift+F10` *(may require pressing* `Fn` *on some devices)*
    - *Run command:* `OOBE\BYPASSNRO` *(this will restart the OOBE if successful)*
    - *Proceed through OOBE like normal until you get to the Network Selection screen*
    - *Select* `I don't have an internet connection` *(if this button is not available the bypass didn't work, proceed to Option 2)*
    - *Select* `Continue with limited setup`
    - *Create a Local Account:* `COPS` (no password)
    - *Complete the OOBE as normal*
  - **Option 2: Internet Connected**
    Force Local Account Creation
    - *Proceed though OOBE like normal until you get to the Login with a Microsoft Account screen*
    - *Open Command Prompt:* `Shift+F10` *(may require pressing* `Fn` *on some devices)*

        - *Run command:* `start ms-cxh:localonly`
        - *Create a Local Account:* `COPS` (no password)

        - *Complete the OOBE as normal*
    - Note regarding Windows 10/11 S Mode
      In some cases you won't be able to open the Command Prompt, you may only see it's black box flash up on the screen and quickly dissapear. This is could be a indication of the Windows 10/11 install being in S Mode (Store Mode), which disables access to terminals (i.e. Command Prompt) and execution of non Microsoft Store apps. If you encounter this, you will not be able create a Local Account during the OOBE, and you will need to complete the OOBE with the customer's Microsoft Account. After the OOBE is complete and you've reached the Windows Desktop environment, you may need to Switch Out of S Mode to proceed with the Data Transfer, as S Mode restricts us from running our tools if required.
        - [OPTIONAL] Switch Out of S Mode
          WARNING: SWITCHING OUT OF S MODE IS A PERMANANT CHANGE AND CANNOT BE REVERTED
            - *Connect to the internet*

            - *Run* `ms-windows-store://pdp/?productid=BF712690PMLF&OCID=windowssmodesupportp`

            - *Follow the prompts to Switch Out of S Mode*
              (this will change the Windows edition installed to Windows 10/11 Home or Pro as per it's installed license)
- **Configure System Restore**

- **Check installed Windows' Edition**

    - *Run* `winver`
- **Create a new System Restore point**
  `COPS - Fresh Windows 10/11 Home/Pro Install` (use 10 or 11 and Home or Pro as per `winver`)
- **Connect to the Internet** (if not already)
- **Check Windows is activated**
  TODO: `ms-settings:activation` or `ms-settings:activation?activationSource=SMC-Article-12440`
- **Configure Time/Date**
- **Configure Windows Update**
    - Open Windows Update
      Run `control update`
    - Click `Resume updates` if updates are currently paused
    - Disable `Get the latest updates as soon as they're available`
    - Advanced options
        - Enable `Receive update for other Microsoft products`

        - Disable `Get me up to date`
        - Enable `Notify me when a restart is required to finish updating`
        - Delivery Optimization
            - Enable `Allow downloads from other devices`
                - Select `Devices on my local network`
- **Update Microsoft Store Apps**

    - Open Microsoft Store
      Run `ms-windows-store:`
        - Click `Downloads`
        - Click `Check for updates`
        - Click `Update all`
- **Update Winget Apps**

    - Open a Terminal
      Run `wt` or `powershell` or `cmd`
    - Run the following commands:
      `winget source update`
      `winget upgrade --all --silent`

- **Update Windows**
- **Update Office apps**

    - Run `"C:\Program Files\Common Files\microsoft shared\ClickToRun\OfficeC2RClient.exe" /update user forceappshutdown=true`
- **Check Drivers**
  Bangs(!) exclamation marks in Device Manager indicates missing, incorrect, or corrupt drivers
    - Open `Device Manager` to check for Bangs(!)
    - Run `Snappy Driver Installer Origin (SDIO)` as an Administrator
    - Select `TODO: Create a new system restore point`
    - Select all missing/incorrect/corrupt drivers (as per bangs! in Device Manager)
    - Click `Install`
- **[OPTIONAL] Update Outdated Drivers**
- **Verify Drivers**
    - **Turn On Windows Verifier:**
        - Run `verifier`
        - Select `Create standard settings`
        - Click `Next`
        - Select `Automatically select all drivers on this computer`
        - Click `Finish`
        - Restart Windows `shutdown -r -f -t 00`

- *Windows Verifier works by stressing out drivers as they're loaded (it is expected that the computer's performance will be impacted while verifier is enabled)*

- *If Windows loads into the desktop OK and does not crash with Verifier enabled, then all is good and you can proceed to turn it off*

- *If Verifier induces a crash, Windows should produce a Blue Screen of Death (BSOD) with a STOP Code error and information on the driver that crashed, you can use this information to identify the faulty driver that caused the crash and replace it*

- **Turn Off Windows Verifier:**
  - Run `verifier`
  - Select `Delete existing settings`
  - Click `Finish`
  - Restart Windows `shutdown -r -f -t 00`

Restore

- **Install Programs**
  - you can use the winget install script for this if you made one - *install programs before restoring the user profile, as otherwise some required registry entries may not exist yet*
- **Restore User Profiles**
  - make Administrator, make default user, set no password and set password does NOT expire
- **Copy over any C: Drive files/folders that were backed up**
- **Restart Windows** (this should log in to the restored user profile)
  - open a command prompt window (or similar) as Administrator to ensure account has admin priviledges
- **Install Printer Drivers**
  - If you can not install the printer drivers + software without the printer present, save the printer package installer to `C:\COPS\` and create a shortcut to it on the customer's desktop
- **Check Web Browsers and restore Bookmarks and Passwords from backups as required**
- **Activate software using extracted keys or accounts as required**
- **Configure email accounts as required**
- **Install additional drivers as required**
- **Move any USB Dongles from the old device (Wireless mice, wifi, blue adapters, etc...)**
- **Update Apps**
  via `Microsoft Store`
  via `Winget`

- **Update Windows**
- **Update Office apps** (if installed)
- **Restart Windows**
- **Remove 'COPS' user account**
  - Run: `netplwiz` - Select `COPS` - Click `Remove`
  - Delete `C:\Users\COPS\` folder
    Windows may prevent you from removing this folder if it's currently accessing it in the background, if this happens just restart Windows and try to remove it again
  - Empty Recycle Bin
- **System Maintenance/Repair**

  - Open a Terminal as Administrator
    Run `wt` or `powershell` or `cmd`
  - Run the following commands:
    ```
    winget source reset --force
    winget source update
    winget upgrade --all --silent
    sfc /scannow
    dism /online /cleanup-image /startcomponentcleanup
    /resetbase
    dism /online /cleanup-image /restorehealth
    sfc /scannow
    defrag /c /o
    chkdsk c: /r /scan /perf
    ```

    Useful Tip
    You can queue up multiple commands in PowerShell by pressing `Shift+Enter` to add a new line before pressing `Enter` to execute the all of the queued up commands one after another
- **Restart Windows**
- **Create a new System Restore point** `COPS - Completed Data Transfer`

Virus/Malware Removal

Windows

Pre Scans

- [**IMPORTANT**] **Air Gap Device** > *Ensure device is disconnected from all networks before RKill is run successfully and RATs (Remote Access Tools) removed, to ensure malicious actors do not re-connect to the device while it's still compromised*

- Enable System Restore (set to 7% allocation if enough free disk space)
- [OPTIONAL] **Create a new System Restore point** `COPS - Pre Virus/Malware Removal` > *This System Restore point will be wiped out in a later step (post-virus/malware removal), as malware can persist in old System Restore points*
- **Restart Windows**
  Force Restart Windows (`shutdown -r -f -t 00`) now to provide a clean environment befor proceeding
- **COPS Folder**
  Create `C:\COPS\` folder on the system
  - [OPTIONAL] Add `C:\COPS\` to the installed antivirus's exclusion list
    Trend Micro
    Windows Security

- **Disable Antivirus**
  Trend Micro
  Windows Security

- **RKill**
  - Copy `RKill` folder from your USB Tool to the `COPS` folder
    RKill can't run from a write-blocked drive, so you'll usually need to copy the executables out first
  - [**IMPORTANT**] Run any RKill executable as Admininstrator
  - Wait for RKill to complete, it will then generate a report `RKill.txt` on the current user's desktop
  - Move `RKill.txt` from `%USERPROFILE%\Desktop` to `COPS` folder
- **Revo Uninstaller**
- **Disk Cleanup**
  - Run `cleanmgr /sageset:10`
    This will open the Disk Cleanup utility to create settings for Profile 10
  - Click `Clean up system files`
  - Select all checkboxes except for the following system error options:
    `System error memory dump files`
    `System error minidump files`
    You can click on an option, and then use the UP + DOWN Arrows + Space Bar to quickly check or uncheck options
  - Click `OK`
  - Run `cleanmgr /sagerun:10`
    This will run the Disk Cleanup utility to using Profile 10's settings

Scans

- Connect to Internet
- [OPTIONAL] AdwCleaner > *AdwCleaner crashes out of UVK's automation, so run it now instead if you want to use it*

- [OPTIONAL] Spybot - Search & Destroy > *Spybot is a thorough malware removal tool, but it can take a very long time to complete it's scans*
- [OPTIONAL] Windows Defender Offline Scan
- [OPTIONAL] Create a new System Restore point `COPS - Pre Virus/Malware Removal`
- Ultra Virus Killer (UVK)
  - Install UVK
  - Open UVK
    - Do not disable Hybrid Shutdown if asked when opening UVK
    - Do Update UVK if asked when opening UVK
  - Click System Repair
  - Select the following repair actions: *(left menu) > (you can click on an option, and then use the UP + DOWN Arrows + Space Bar to quickly check or uncheck options)*
    - **Pre-Repair Actions** 1. Set technician power settings 2. Kill all non system processes 3. Delete all restore points 4. Create a system restore point 5. Free physical memory 6. Backup the registry 7. Un-immunize all areas 8. Disable the User Account Control 9. Enable the legacy (F8) boot menu 10. Enable Windows Recovery Environment 11. Prevent rebooting until all is done
    - **Third-Party Built-in Apps** 12. Ultra Adware Killer scan 13. MalwareBytes AntiMalware scan 14. Super AntiSpyware scan 15. RogueKiller scan 16. Kaspersky TDSSKiller scan 17. Avast! Browser Cleanup
    - **Reset Actions** 18. Reset the DNS cache 19. Reset the Windows Store 20. Reset all print jobs
    - **Fixes for Common Windows Problems** *n/a*
    - **File System Related Actions** 21. Rebuild icon cache
    - **Essential Installes/Updates** [If Google Chrome is installed] 22. Insall/Update Chrome 23. Install uBlock Origin for Chrome [If Mozilla Firefox is installed] 24. Install/Update Firefox 25. Install uBlock Origin for Firefox 26. Install uBlock Origin for Edge 27. PatchMyPC - Update all apps
    - **Privacy Cleanup** 28. Clear all browsers history (all users) 29. Delete browsers cookies (all users)
    - **Maintenance Actions** 30. Empty all users temp folders 31. Empty browsers cache (all users) 32. Unattended disk cleanup
    - **System Repair and Optimization** n/a
    - **Windows Troubleshooters** n/a
    - **Post-Repair Actions** 33. Restore the previous UAC state 34. Restore previous immunization 35. Delete all restore points (post repair) 36. Create restore point (post repair) 37. Reset power settings 38. Uninstall Malwarebytes Antimalware 39. Uninstall Super AntiSpyware 40. Uinstall RogueKiller 41. Uninstall this application 42. Restore

normal boot
- Select the following loadout settings: *(right menu)* 1. Third party full scans 2. Use unattended mode
- Click `Run selected fixes/apps`

Post Scans

- [OPTIONAL] Create a new System Restore point "**COPS - Pre Windows Update**"
- Update Windows (no preview updates)
- Update Apps via Microsoft Store
- Update Apps via Windows Package Manager (winget) `winget source update`
  `winget upgrade --all --silent`

  Tip
  You can queue up multiple commands in PowerShell by pressing `Shift+Enter` to add a new line before pressing `Enter` to execute the all of the queued up commands one after another
- [OPTIONAL] Create a new System Restore point "**COPS - Pre Driver Update**"
- Update Drivers (SDIO)
- Verify Drivers
  - **Turn On Windows Verifier:**
    - Run `Win+R`: `verifier`
    - Select `Create standard settings`
    - Click `Next`
    - Select `Automatically select all drivers on this computer`
    - Click `Finish`
    - Restart Windows (`shutdown -r -f -t 00`)
      Windows Verifier works by stressing out drivers as they're loaded (it is expected that the computer's performance will be impacted while verifier is enabled)
      If Windows loads into the desktop OK and does not crash with verifier enabled, then all is good and you can proceed to turn it off
  - **Turn Off Windows Verifier:**
    - Run `Win+R`: `verifier`
    - Select `Delete existing settings`
    - Click `Finish`
    - Restart Windows (`shutdown -r -f -t 00`)
- **System Maintenance/Repair**

  - Open a Terminal as Administrator
    Run `wt` or `powershell` or `cmd`

- Run the following commands:
  ```
  winget source reset --force
  winget source update
  winget upgrade --all --silent
  sfc /scannow
  dism /online /cleanup-image /startcomponentcleanup
  /resetbase
  dism /online /cleanup-image /restorehealth
  sfc /scannow
  defrag /c /o
  chkdsk c: /r /scan /perf
  ```

  Useful Tip
  You can queue up multiple commands in PowerShell by pressing `Shift+Enter` to add a new line before pressing `Enter` to execute the all of the queued up commands one after another
- Create a new System Restore point `COPS - Post Virus/Malware Removal`

Android

Pre Scans

- **Remove Intrusive Full-Screen Pop-Ups**
  These relentless pop-ups make the device impossible to work with, so deal with these first *(if applicable)*

  More Info
  These full screen pop-ups/ads aren't a sign of an injection, but merely a malicious use of the native Android notification system.
  Users don't intentionally give these apps permission to do this, but it's often caused by Tapjacking or simply users ignorantly agreeing to permission prompts.
  - Open `Play Store`
    - Install Ad Virus Cleaner - ROX Security
  - Open `ROX Security`
    - Tap `Scan`
    - Wait for the scan to complete
    - Tap on `Pop-up Ad Detector`
      - Tap on `Give Permissions`
        This will open a required permissions settings panel
        - Enable `ROX Security`
        - Tap `<` *(back button)*
    - Wait for an intrusive full-screen pop-up

        - Tap `|||` *(app switch button)*
            - Switch back to `Rox Security` `Rox Security` should have logged recent app activity under it's `Pop-up Ad Detector`
        - Tap `:` *(kebab button)* next to the offending app
            - Tap `Show in Play Store`
            - Verify the app is not important
              If the app is published by Google or the device's manufacturer (i.e. Samsung) think twice before removing
            - Tap `Uninstall`
    - Uninstall `ROX Security` when done
- **Safe Mode**
  Reboot the device in Safe-Mode *(if available)*
- **Malicious or Suspicious Apps**

    - Remove any remote access apps *(i.e. AnyDesk, TeamViewer, etc..)*
      These are used by scammers to access devices remotely
    - Remove any malicious or bloatware apps
      The following are common types of apps that are unnecessary often load their own malware:
        - Any free 3rd-party "cleaner" apps
        - Any free 3rd-party "QR Scanner" apps
        - Any free 3rd-party "PDF Reader" apps *(excluding Adobe Acrobat Reader)*
        - Any free 3rd-party "File Manager" apps
    - Remove any "Crypto" apps *(after verifying the customer does not genuinely use them)*
      Scammers often load on crypto apps to try and steal currencies the device has access to
- **Web Browsers**
  Clear Cache + Data for all Web Browsers installed on the device.
  The following steps are for Google Chrome, but other apps are managed that same way
    - Open `Settings`
        - Tap `Apps`
            - Tap `Chrome`
                - Tap `Storage`
                    - Tap `Clear cache`
                    - Tap `Clear data`

1st Party Scans

- `Play Protect` Scan
- [If Samsung Device]
    - Samsung `Device Care` Scan

3rd Party Scans

- Install and Run at least 3 of the following free malware scanners:
  - Malwarebytes Mobile Security
  - AVG AntiVirus & Security
  - Bitdefender Antivirus
  - Sophos Intercept X for Mobile
  - Avira Security Antivirus & VPN
  - Trend Micro Mobile Security & Antivirus
  - ESET Mobile Security Antivirus
  - TotalAV Mobile Security *untested if can be used without an account*
  - Panda Dome Antivirus and VPN *untested if can be used without an account*
  - Avast Antivirus & Security *untested if can be used without an account*

Updates

- Update Apps via `Play Store`
- [If Samsung Device]
  - Update Apps via `Galaxy Store`
- Update `Android OS`
  This may take multiple updates and reboots, as customers often neglect updating their devices

Backup / Export

Windows

macOS

Backup Device

- Use Time Machine

iOS

Export Messages

- imessage-exporter

Export Photos

- Connect the iOS device to a macOS device
  You may need to unlock the iOS device and tap `Trust` if prompted
- Open `Image Capture` app

- Click on the iOS device
  The connected iOS device should show up under `DEVICES` on the left
- Change `Import To:` folder
  Make a Job# folder to import the photos/videos to
- Click `Download All`

Backup iCloud Photos

- Submit `Apple Privacy Data Request`
  - Sign in Apple's Data and Privacy page with the customer's `Apple Account`
  - Click `Request a copy of your data`
  - Tick `iCloud Photos`
  - Click `Continue`
  - Choose the largest bundle/zip size *(this will make downloading the files easier, as you can only download 3 of the part files at a time)*
- Check confirmation email
  Apple will send a confirmation email to the customer's Apple Account email address, if this does not come through now then you may have issues receiving the download link email later
- Wait for the download link email
  Apple will have to compile and zip up all of the data you requested, this can take many days
- Open download link
- Download all .zip files Apple prepared for download
- Unzip all .zip files
- Combine the unzipped data in to one folder

Android

OS Install Media Creation

Windows

Download

- Download from massgrave.dev

Verify

- Verify checksums against rg-adguard.net

Flash

- Flash image to USB using Rufus
  `winget install rufus.rufus`

Inject Drivers

Prep

- Have a folder with extracted drivers ready to go
  `C:\drivers\` for this example
- Create an empty directory ready to mount the Windows image to for editing
  `C:\mount\` for this example
- Have a Windows image ready to go
  `F:\sources\install.wim` for this example

Mount

- Open Powershell as admin
- Find index of the Windows image you want to mount
  `Get-WindowsImage -ImagePath F:\sources\install.wim`
- `Mount-WindowsImage -Path C:\mount\ -ImagePath F:\sources\install.wim -Index 1`

Add Drivers

- `Add-WindowsDriver -Path C:\mount\ -Driver C:\drivers\ -Recurse -ForceUnsigned`

Unmount

- `Dismount-WindowsImage -Path C:\mount\ -Save`

Sideloading

Android

Download

- Download desired .APK from 3rd party source or directly from the `Google Play` store using Aurora Store
- [If you can only download an App Bundle (.APKS, .XAPK, .APKM)]
  - Use AntiSplit M to merge the bundle components back in to a .APK file

Upload

- Connect the Android device to a computer
- Navigate to it's mounted file system *(i.e. in `This PC`)*
- Open `Downloads` folder
- Copy `.APK` file in to the `Downloads` folder

Install

- Enable Sideloading
  Depending on the manufacturer of the device, you may need to enable Sideloading before you can install .APK files.
  Samsung
- Open `Files` app
- Navigate to `Downloads` folder
- Tap on the `.APK` file
- Tap `Install`

USB Tool

Ventoy

Medicat

Bootable Tools

Windows Tools

COPS Extras (scripts, etc..)