Laptop Instructions

For Bloomberg Issued PC Laptops

Bloomberg

Before you begin, ensure that:

- You have enrolled your B-Unit or set up the Android B-Unit.
- For new hires, you (re)set" your CORP password via CHPW <GO> in the Bloomberg Terminal®.
- For existing employees, your CORP password has not expired. If the password expired or you forgot it, use CHPW <GO> to reset your CORP password in the Bloomberg Terminal®..

Laptop Tips

Personnel must adhere to the following requirements when using a Laptop:

- Except as otherwise authorized, users shall not disable or bypass security controls or the established request and approval processes. Examples of prohibited actions include, but are not limited to, disabling antivirus programs, disabling device
- Restricted Client Data (as defined in the Data Classification and Handling Standard) shall not be stored on laptops.
- Except as otherwise authorized, data shall not be copied from Laptops to removable media devices or to non-Bloomberg devices and systems.
- Only software approved through the BOSS <GO> process shall be installed on Laptops, and the software installation shall be done by the Information Systems Department ("InfoSys").
- Users shall not alter Laptop network configurations, including firewall rules, routes, etc.
- Laptops are the property of Bloomberg and shall be returned to Bloomberg upon request or when no longer needed.
- Lost Laptops must be reported immediately by submitting an SDSK ADD 29008 <GO> ticket for "Mobile/Lost or Stolen Mobile Device."

Please refrain from putting stickers on your laptop, especially ones that identify this as a Bloomberg-owned laptop.

Do not tape passwords or login information to the laptop.

Reboot your laptop weekly to ensure updates are applied.

When you finish orientation and acclimate to the terminal, you can access this information at: {POLYID:3606497<GO>}

PC Laptop Instructions

Setup

Initiate

1. Power on the laptop, then select your language and keyboard preferences.
2. Connect to a network. You **MUST CONNECT** to a WiFi network prior to advancing. Once connected to a network, click **NEXT**.

Install Profiles

3. Enter your CORP PC login username with the extension of @bloomberg.com on the Microsoft email page. Example: *jdoe@bloomberg.com*
4. Enter your corporate PC username and password on the Bloomberg Single Sign On page (BSSO) *(you do not need to enter @bloomberg.com, just your username i.e., jdoe).*
5. Enter your six-digit token when prompted. This is obtained by swiping your finger on the B-Unit, or via the Android B-Unit app.
6. Wait for the profile to install. Three profiles will install automatically and can take anywhere between 10-15 minutes each, depending on your network speed. Once installation is complete, you are logged into a Windows desktop. If the account setup fails, select Continue Anyway to proceed. Do not select Try Again.

Finish

7. Launch the Bloomberg Application. Use your Bloomberg Terminal® username, password, and B-Unit to gain access.

Compliance Check — Ensure disk encryption is active. Important to check before using your laptop.

8. Right-click **Windows Start**, then select **Windows Powershell (Admin)**. When you see the popup, click **Yes**. The *Windows Powershell Admin* window appears.
9. Enter the following command: **manage-bde c: -status**
   – Ensure *Percentage Encrypted* is 100.0%.
   – Ensure *Protection Status* is set to **Protection On**.
10. If *Percentage Encrypted* is NOT 100.0%:
    – Enter the following command: **manage-bde c: -pause**
    – Enter the

Bloomberg

following command: **manage-bde c: -resume**

Percentage Encrypted should move up to 100.00% in a few minutes.

11. If *Percentage Encrypted* is 100.0% but *Protection Status* is set to **Protection Off**, then run the following Bitlocker procedure:
    – Open *File Explorer* and click **This PC**.
    – Right-click on C: drive and select **Enable Bitlocker**.
    – Select **Activate BitLocker**. Once Activation completes, close the Bitlocker window.
    – Go back to *Window Powershell Admin* window and refresh your **manage-bde c: -status** command to verify **Protection = ON**.
    – Close *Windows Powershell Admin* window.

If you need additional support, contact our support team by scanning the QR below, which brings you to a web page with our global support phone numbers.

Version 1.0