JT

TPM 2.0 and Secure Boot by Brand

Practical computer help written for everyday users

Safety: Back up important data when possible. Power off and unplug equipment before opening a computer. Stop if you see liquid damage, smoke, burning smell, or a failing drive.

Before entering BIOS

• Press Win+R, run tpm.msc, and check Specification Version.

• Run msinfo32 and check BIOS Mode and Secure Boot State.

• Suspend BitLocker before firmware changes if device encryption is active.

ASUS

• AMD: Advanced Mode > Advanced > AMD fTPM Configuration > AMD CPU fTPM.

• Intel: Advanced > PCH-FW Configuration > Intel Platform Trust Technology (PTT).

MSI

• Settings > Security > Trusted Computing > Security Device Support. Choose AMD CPU fTPM or Intel PTT when shown.

Gigabyte / AORUS

• AMD: Settings > AMD CPU fTPM.

• Intel: Settings > Miscellaneous or Trusted Computing > Intel Platform Trust Technology.

ASRock

• Security > Trusted Computing > Security Device Support. Select AMD fTPM or Intel PTT when available.

Dell

• Security > TPM 2.0 Security. Enable TPM On and activation options.

HP

• Security or System Security > TPM Embedded Security / TPM Device. Set to Available or Enabled.

Lenovo

• Security > Security Chip. Enable Intel PTT, AMD Platform Security Processor, or Security Chip 2.0.

Acer

• Security > Trusted Computing or TPM. Some models require setting a temporary Supervisor Password before options appear.

Important

• Exact labels vary by model and BIOS revision. Never interrupt a BIOS update. Save recovery keys before changing TPM or Secure Boot settings.

This guide is educational and cannot identify every hardware or data-loss risk remotely. Use the exact manual for your device or motherboard when firmware settings differ.