If you want your system to require a PIN number in order to unlock a Bitlocker encrypted drive at boot time, you need to change one small GPO setting (assuming that you have Bitlocker already set up):

Start Group Policy editor by pressing Windows+R and entering the command 'gpedit.msc'

	Run ×			
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.			
<u>O</u> pen:	gpedit.msc 🗸			
	OK Cancel <u>B</u> rowse			

Start the Local Group Policy Editor

Navigate to Local Computer Policy \rightarrow Computer Configuration \rightarrow Administrative Templates \rightarrow Windows Components \rightarrow Bitlocker Drive Encryption \rightarrow Operating System Drives

Local Group Policy Editor –							
Action View Help							
🔶 🚈 🖬 🔀 🖬 🍸							
Windows Components ActiveX Installer Service	🚊 Operating System Drives /						
Add features to Windows 8.1	Require additional authentication at startup	Setting	State	Comment			
App Package Deployment		E Allow network unlock at startup	Not configured	No			
App runtime	Edit policy setting	E Allow Secure Boot for integrity validation	Not configured	No			
Application Compatibility	Cure policy secting	Require additional authentication at startup	Enabled	No			
AutoPlay Policies	Requirements:	🗄 Require additional authentication at startup (Windows Serve	Not configured	No			
Biometrics	At least Windows Server 2008 R2	🗄 Disallow standard users from changing the PIN or password	Not configured	No			
a 📋 BitLocker Drive Encryption	or Windows / Description: This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform	Enable use of BitLocker authentication requiring preboot ke	Not configured	No			
Fixed Data Drives		E Allow enhanced PINs for startup	Not configured	No			
Operating System Drives		Configure minimum PIN length for startup	Not configured	No			
Removable Data Drives		🗄 Configure use of hardware-based encryption for operating s	Not configured	No			
Credential User Interface		Enforce drive encryption type on operating system drives	Not configured	No			
Desktop Gadgets		E Configure use of passwords for operating system drives	Not configured	No			
Desktop Window Manager		E Choose how BitLocker-protected operating system drives ca	Not configured	No			
Device and Driver Compatibility	Module (TPM). This policy setting	E Configure TPM platform validation profile for BIOS-based fi	Not configured	No			
	BitLocker. Note: Only one of the additional	🗄 Configure TPM platform validation profile (Windows Vista,	Not configured	No			
Edge Of		E Configure TPM platform validation profile for native UEFI fir	Not configured	No			
Event Log Service		E Reset platform validation data after BitLocker recovery	Not configured	No			
Event Viewer	authentication options can be	📰 Use enhanced Boot Configuration Data validation profile	Not configured	No			
Family Safety	policy error occurs.						
File Explorer	V						
A en una	If you want to use Bitl ocker on a						
>	\ Extended _\ Standard /						

Navigate to 'Operating System Drives'

Select the 'Require additional authentication at startup' option, and set it to 'Enabled'. Then set 'Configure TPM startup PIN' to 'Require startup PIN with TPM'

Require additional authentication at startup – 🗖 🗙						
Require additional authentication at startup Previous Setting						
 Not <u>C</u>onfigured <u>E</u>nabled <u>D</u>isabled 	Comment: Supported on:	At least Windov	ws Server 2008 R2 or Windows 7			
Options:			Help:			
Allow BitLocker without a compatible TPM (requires a password or a startup key on a USB flash drive) Settings for computers with a TPM: Configure TPM startup: Allow TPM Configure TPM startup PIN: Require startup PIN with TPM Configure TPM startup key: Allow startup key with TPM Configure TPM startup key and PIN: Allow startup key and PIN with TPM Configure TPM startup key and PIN: Allow startup key and PIN with TPM Configure TPM startup key and PIN: Configure TPM startup key and PIN with TPM Configure TPM startup key and PIN: Configure TPM startup key and PIN with TPM configure TPM startup key and PIN k			 This policy setting allows you to configure whether BitLocker requires additional authentication each time the computer starts and whether you are using BitLocker with or without a Trusted Platform Module (TPM). This policy setting is applied when you turn on BitLocker. Note: Only one of the additional authentication options can be required at startup, otherwise a policy error occurs. If you want to use BitLocker on a computer without a TPM, select the "Allow BitLocker without a compatible TPM" check box. In this mode either a password or a USB drive is required for start-up. When using a startup key, the key information used to encrypt the drive is stored on the USB drive, creating a USB key. When the USB key is inserted the access to the drive is authenticated and the drive is accessible. If the USB key is lost or unavailable or if you have forgotten the password then you will need to use one of the BitLocker recovery options to access the drive. On a computer with a compatible TPM, four types of 			
			OK Cancel Apply			

Set 'Configure TPM startup pin' to 'Require startup PIN with TPM'

Now open CMD in elevated mode and enter the command to set the PIN

manage-bde -protectors -add c: -TPMAndPIN

This will prompt you for a PIN which You will enter at Boot time.

