ThinkPad

ThinkPad USB 3.0 Secure Hard Drive User Guide

1 http://www.lenovo.com/safety

Note: Before installing the product, be sure to read the warranty information in Appendix B "Lenovo Limited Warranty" on page 15.

Fourth Edition (August 2013)

© Copyright Lenovo 2011, 2013.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Contents

Chapter 1. About the secure hard		
drive		1
Product description.		1
Overview		2
Chapter 2. Installing the secure hard drive		3
	•	-
Before you begin.	·	3
Installing the secure hard drive	·	3
Chapter 3. Using the secure hard		
drive		5
Entering and exiting the working modes		5
Entering standby mode		5
Entering administrator mode		5
Exiting administrator mode		5
Entering user mode		6
Exiting user mode		6
Password management		6
Changing the administrator password.		6
Adding a new user password		7
Changing the user password		7
Deleting the user password(s)		8
Lock the secure hard drive		8
Manually lock the secure hard drive		8
Lock the secure hard drive with the auto-lock function		8
Hibernating, suspending, or logging off from the operating system.		9
Completely resetting the secure hard drive		9
Initializing and formatting the secure hard drive after a complete reset		9

Chapter 4. Troubleshooting	11
Appendix A. Service and Support	13
Online technical support	13
Telephone technical support	13
Appendix B. Lenovo Limited	
Warranty.	15
Part 1 - General Terms	15
Part 2 - Country-specific Terms	17
Part 3 - Warranty Service Information	20
Suplemento de Garantía para México	21
Appendix C. Electronic emission	
notices	23
Federal Communications Commission Declaration	
of Conformity	23
Appendix D. Notices	27
Recycling information	27
Recycling information for Brazil	27
Export Classification Notice	28
Trademarks	28
Appendix E. Restriction of Hazardous	
Substances Directive (RoHS)	29
European Union RoHS	29
China RoHS	29
	29
Ukraine RoHS	29
India RoHS	29

Chapter 1. About the secure hard drive

This chapter provides product information about the ThinkPad USB 3.0 Secure Hard Drive (hereafter called the secure hard drive).

Product description

The secure hard drive is a portable, light-weight, and high-speed USB (Universal Serial Bus) 3.0 standard option that offers high-level data security. You can transfer data using the integrated USB cable on the secure hard drive or the provided USB 3.0 Y cable. In addition to regular USB 3.0 hard disk drive functions, it also provides you with an easy-to-use full disk encryption solution. All the functions are integrated into the secure hard drive; therefore, you can access the secure hard drive and manage passwords without using other software applications.

The secure hard drive has three working modes: standby mode, administrator mode, and user mode. For more information about the working modes, refer to Chapter 3 "Using the secure hard drive" on page 5.

Note: Passwords are required for administrator mode and user mode. Accordingly, they are called the administrator password and the user password.

Your option package includes the following:

- ThinkPad USB 3.0 Secure Hard Drive
- USB 3.0 Y cable
- Carrying case
- · Setup and warranty poster

Overview

The following figure shows the overview of the secure hard drive.

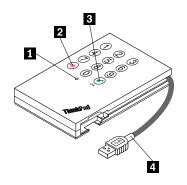


Figure 1. Overview of the secure hard drive

1 Status LED (light-emitting diode)	The status LED indicates the working modes:		
	Red: standby mode		
	Blue: administrator mode		
	Green: user mode		
	For more information about the working modes and the status LED, refer to Chapter 3 "Using the secure hard drive" on page 5.		
2 🔀 button	Use this button to do the following:		
	Canceling the current operation		
	Returning to the previous step when you accidently input a wrong password		
	Exiting administrator mode and user mode		
	Manually locking the secure hard drive		
3 🖍 button	Use this button to access the secure hard drive or give an OK acknowledgement for the following operations:		
	Inputting a password		
	Confirming a new password		
4 Integrated USB cable	You can connect the secure hard drive to your computer using the integrated USB cable. For more information, refer to "Installing the secure hard drive" on page 3.		

Chapter 2. Installing the secure hard drive

This chapter provides information about how to install the secure hard drive.

Before you begin

Be sure to carefully read the following information before installing and using the secure hard drive.

Attention:

- Make sure that you use the integrated USB cable on the secure hard drive or the provided USB 3.0 Y cable to install the secure hard drive. Using any cables other than the two cables might damage the secure hard drive.
- Carefully handle the secure hard drive. When the secure hard drive is not in use or you need to ship it to a different location, place it in the provided carrying case.
- To get reliable performance of the secure hard drive, make sure that the integrated USB cable on the secure hard drive or the provided USB 3.0 Y cable is connected to the USB connectors on your computer or to an ac-powered USB hub. Do not connect the two cables to a non-ac-powered USB hub.

Installing the secure hard drive

To install the secure hard drive, do one of the following:

• Connect the integrated USB cable on the secure hard drive to a USB 2.0 or USB 3.0 connector on your computer. When the connection is established, the status LED turns red.

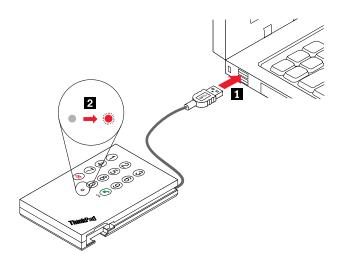


Figure 2. Installing the secure hard drive using the integrated USB cable

 Connect the USB receptacle connector of the USB 3.0 Y cable to the integrated USB cable on the secure hard drive, and then connect the two USB connectors at the other end of the USB 3.0 Y cable to two USB 2.0 or USB 3.0 connectors on your computer. When the connection is established, the status LED turns red.

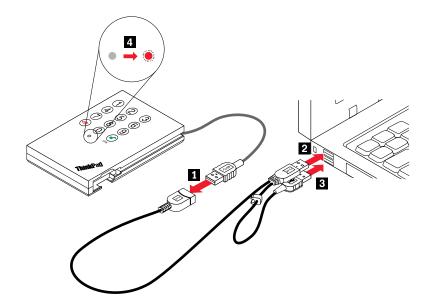


Figure 3. Installing the secure hard drive using the USB 3.0 Y cable

Note: For computers with USB 3.0 connectors, you can connect the secure hard drive to a USB 3.0 connector on the computer using only the main connector of the USB 3.0 Y cable. For computers with only USB 2.0 connectors, to ensure sufficient power supply, it is recommended that you connect both the main connector and the additional power supply connector of the USB 3.0 Y cable to the computer.

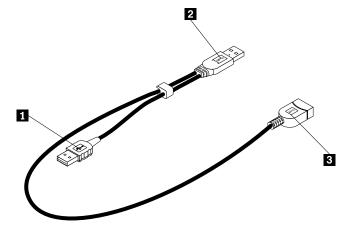


Figure 4. Overview of the USB 3.0 Y cable

1 Additional power supply connector

2 Main connector

3 USB receptacle connector

Chapter 3. Using the secure hard drive

This chapter provides information about how to use the secure hard drive.

Entering and exiting the working modes

This section provides information about how to enter and exit standby mode, administrator mode, and user mode of the secure hard drive.

Entering standby mode

Standby mode is the default working mode of the secure hard drive. In this mode, the secure hard drive is locked; therefore, it cannot be recognized by the operating system. However, standby mode enables you to enter and switch between administrator mode and user mode.

To enter standby mode, connect the secure hard drive to your computer. When the status LED turns red, it indicates that the secure hard drive goes into standby mode. For more information about how to connect the secure hard drive, refer to "Installing the secure hard drive" on page 3.

Note: To switch between administrator mode and user mode, you are required to firstly switch to standby mode, and then you can enter your desired mode.

Entering administrator mode

In administrator mode, you can change the administrator password, create up to 10 user passwords, delete all user passwords, and set the auto-lock function. For more information, see "Password management" on page 6 and "Lock the secure hard drive with the auto-lock function" on page 8. The secure hard drive is locked in this mode; therefore, it cannot be recognized by the operating system.

To enter administrator mode, do the following:

- 1. Connect the secure hard drive to your computer. When the status LED turns red, it indicates that the secure hard drive goes into standby mode. For more information about how to connect the secure hard drive, refer to "Installing the secure hard drive" on page 3.
- 2. Hold **●**+0 for five seconds until the status LED flashes in red. This indicates that you can input the administrator password.
- 3. Input the administrator password and press

 to enter administrator mode. The default administrator password is 12345678. When the status LED turns blue, it indicates that the secure hard drive goes into administrator mode.

Note: If the status LED flashes in red for a few seconds after you input the administrator password, it indicates that the secure hard drive has returned to standby mode. You need to go back to step 2 to enter administrator mode again. This problem is caused by one of the following reasons:

- An incorrect administrator password is input in step 3.
- No activity is detected within two minutes in administrator mode.

Exiting administrator mode

To exit administrator mode, hold *X* until the status LED turns red. The secure hard drive goes into standby mode.

Entering user mode

In user mode, you can access the secure hard drive and change the current user password. The secure hard drive is unlocked in this mode; therefore, you can use it to transfer data.

To enter user mode, do the following:

- 1. Connect the secure hard drive to your computer. When the status LED turns red, it indicates that the secure hard drive goes into standby mode. For more information about how to connect the secure hard drive, refer to "Installing the secure hard drive" on page 3.

Notes:

- If you incorrectly input the user password or the administrator password six consecutive times, the secure hard drive will no longer respond and the status LED will turn off. You need to disconnect the secure hard drive, and then reconnect it to your computer for additional password attempts.
- If you incorrectly input the user password or the administrator password 25 consecutive times, the secure hard drive will be locked and the status LED will quickly flash in red. To unlock the secure hard drive, do the following:
 - 1. Disconnect the secure hard drive from your computer.
 - 2. Hold 5 while reconnecting the secure hard drive to your computer. The status LED alternately flashes in red and in green.
 - 3. Press 5278879. The status LED turns red, indicating that the secure hard drive is unlocked for additional password attempts.
- If you incorrectly input the user password or the administrator password 50 consecutive times, the secure hard drive will be locked and the status LED will quickly flash in red. The secure hard drive has to be completely reset and then formatted. For more information, see "Completely resetting the secure hard drive" on page 9 and "Initializing and formatting the secure hard drive after a complete reset" on page 9.

Exiting user mode

Attention: Be sure to save all documents on the secure hard drive before exiting user mode.

To exit user mode, do one of the following:

- Hold 🔀 until the status LED turns red.
- Click the **Safely Remove Hardware** icon in the notification area on your computer screen. A message will be displayed, prompting you that you can safely disconnect the secure hard drive from your computer. Then, depending on your operating system, the status LED stays in green or turns red. You can choose whether to disconnect the secure hard drive or not.

Note: It is not recommended to exit user mode when the secure hard drive is transferring data.

Password management

This section provides information about managing your administrator password and user password.

Changing the administrator password

To change the administrator password, do the following:

- 1. Enter administrator mode. See "Entering administrator mode" on page 5 for more information.
- 2. Hold **I**+9 until the status LED flashes in blue.
- 3. Input a new administrator password (a minimum of eight digits and a maximum of 16 digits), and then press **●**. The status LED flashes in green three times.

Note: If the status LED flashes in red three times, it indicates that the new administrator password is less than eight digits or more than 16 digits. After the status LED flashes in blue, input an administrator password that contains eight to 16 digits.

4. Input the new administrator password again, and then press **■**[^]. The status LED stays in green for three seconds, indicating that the administrator password is successfully changed.

Notes:

- If the status LED flashes in red three times and then flashes in blue, go back to step 3. This problem is caused by one of the following reasons:
 - You wait longer than 10 seconds before inputting the new administrator password.
 - The new administrator password is incorrectly input.
- If no activity is detected within two minutes in administrator mode, the secure hard drive will return to standby mode.

Adding a new user password

The secure hard drive enables you to have up to 10 user passwords. To add a new user password, do the following:

- 1. Enter administrator mode. See "Entering administrator mode" on page 5 for more information.
- 2. Hold **I**+1 until the status LED flashes in blue.
- Input a new user password (a minimum of eight digits and a maximum of 16 digits), and then press
 The status LED flashes in green three times.

Note: If the status LED flashes in red three times, this indicates that the new user password is less than eight digits or more than 16 digits. After the status LED flashes in blue, input a user password that contains eight to 16 digits.

Notes:

- If the status LED flashes in red three times and then flashes in blue, go back to step 3. This problem is caused by one of the following reasons:
 - You wait longer than 10 seconds before inputting the new user password.
 - The new user password is incorrectly input.
- If no activity is detected within two minutes in administrator mode, the secure hard drive will return to standby mode.

Changing the user password

Note: If you have more than one user password, you can change only one user password at a time.

To change the user password, do the following:

- 1. Enter user mode. See "Entering user mode" on page 6 for more information.
- 2. Hold **I**⁺¹ for five seconds until the status LED flashes in red.

Note: If the status LED flashes in red, go back to step 2. This problem is caused by one of the following reasons:

- You wait longer than 10 seconds before inputting the new user password.
- The current user password is incorrectly input.

Note: If the status LED flashes in red three times, this indicates that the new user password is less than eight digits or more than 16 digits. After the status LED flashes in blue, input a user password that contains eight to 16 digits.

5. Input the new user password again, and then press ■. The status LED stays in green, indicating that the user password is successfully changed.

Note: If the status LED flashes in red three times and then flashes in blue, go back to step 4. This problem is caused by one of the following reasons:

- You wait longer than 10 seconds before inputting the new user password.
- The new user password is incorrectly input.

Note: The administrator password can be used as a user password. An administrator password can be changed only in administrator mode. For more information, see "Changing the administrator password" on page 6.

Deleting the user password(s)

To delete the user password(s), do the following:

- 1. Enter administrator mode. See "Entering administrator mode" on page 5 for more information.
- 2. Hold 7+8+ for five seconds until the status LED flashes in blue. After that, the status LED flashes in green three times, and then flashes in blue.
- 3. Hold 7+8+■[^] for five seconds again until the status LED becomes green for three seconds and then turns blue. This indicates that the user password(s) are successfully deleted.

Attention: If you have more than one user password, all user passwords will be deleted at a time.

Lock the secure hard drive

To ensure the data security of your secure hard drive when you are away from your computer, you can manually lock the secure hard drive or use the auto-lock function.

Manually lock the secure hard drive

To manually lock the secure hard drive, hold X until the status LED turns red.

Lock the secure hard drive with the auto-lock function

If there is no data transmission after an auto-lock interval, which you need to set in advance, the secure hard drive will lock itself. Then, the status LED will turn red, and you will not be able to access the secure hard drive unless you unlock it by inputting the correct user password and then press r.

To set the auto-lock interval, do the following:

1. Enter administrator mode. See "Entering administrator mode" on page 5 for more information.

- 2. Hold **I**⁺+6 until the status LED alternately flashes in red and in blue.
- 3. Set the auto-lock interval by pressing the following numeric keys:
 - **0**: If you press this numeric key, the auto-lock function will be disabled.
 - 1: If you press this numeric key, the auto-lock interval will be five minutes.
 - 2: If you press this numeric key, the auto-lock interval will be 10 minutes.
 - 3: If you press this numeric key, the auto-lock interval will be 20 minutes.

Note: By default, the auto-lock function is disabled.

Note: Be sure to save all documents on the secure hard drive before the secure hard drive locks itself. If any document is not saved before the secure hard drive locks itself, a message box will be displayed, reminding you that the document directory cannot be found. You need to unlock the secure hard drive to save the document.

Hibernating, suspending, or logging off from the operating system

Before hibernating, suspending, or logging off from the operating system, do the following:

- 1. Save and close all the files on the secure hard drive.
- 2. Click the **Safely Remove Hardware** icon in the notification area on your computer screen. Then, a message is displayed, prompting you that you can safely disconnect the secure hard drive from your computer. You can choose whether to disconnect the secure hard drive or not.

Note: To ensure the data integrity of your secure hard drive, be sure to lock or disconnect your secure hard drive if you are away from your computer or you are sharing your computer with others using different Windows[®] user accounts.

Completely resetting the secure hard drive

If you forget all user passwords or the administrator password, you can perform a complete reset to delete all user passwords, and restore the administrator password to 12345678.

Attention: Completely resetting the secure hard drive will erase all the data on the secure hard drive. You need to initialize and format the secure hard drive with the disk management application. For more information, see "Initializing and formatting the secure hard drive after a complete reset" on page 9.

To completely reset the secure hard drive, do the following:

1. Hold 🔀 while you connect the secure hard drive to your computer. The status LED alternately flashes in blue and in red.

Note: If no activity is detected for 30 seconds in this step, the secure hard drive will go into standby mode.

- 2. Hold ≪X+1+2 for 10 seconds until the status LED turns green for three seconds. The complete reset finishes.
- 3. Disconnect the secure hard drive from your computer.

Initializing and formatting the secure hard drive after a complete reset

A complete reset of the secure hard drive will erase all information and partition settings on the secure hard drive. You need to initialize and format the secure hard drive after a complete reset.

Attention: It is not recommended to initialize and format the secure hard drive on a Microsoft[®] Windows XP operating system because this might decrease the writing speed of the secure hard drive.

To initialize and format the secure hard drive, do the following:

For the Windows XP, Windows Vista, or Windows 7 operating system:

- 1. After a complete reset, connect the secure hard drive to your computer.
- 2. Input the default user password 12345678, and then press ildot to enter user mode. The operating system automatically installs all the USB device drivers for the secure hard drive.
- 3. Depending on your Start mode, click Start.
- 4. Right-click **My Computer** or **Computer**, and then click **Manage**. The Computer Management window opens.
- 5. In the Computer Management window, click **Disk Management**. The Disk Management window opens, and the secure hard drive is recognized as an unknown device that is uninitialized and unallocated.
- 6. For Windows XP: the Initialize and Convert Disk Wizard window opens, click $Next \rightarrow Next \rightarrow Finish$.

For Windows Vista and Windows 7: the Initial Disk window opens, click **OK** with default MBR partition.

Notes: If the Initialize and Convert Disk Wizard window does not open, do the following:

- a. Right-click Unknown Disk, and then select Initialize Disk.
- b. In the Initialize Disk window, click **OK**.
- 7. For Windows XP: Right-click your mouse in the blank area of the unallocated device section, and then select **New Partition**. The Welcome to the New Partition Wizard window opens.

For Windows Vista and Windows 7: Right-click your mouse in the blank area of the unallocated device section, and then select **New Simple Volume**. The Welcome to the New Simple Volume window opens.

- 8. Click Next \rightarrow Next \rightarrow Next.
- 9. Input a name for the volume label and select **Perform a quick format**. Then, click **Next**.
- 10. Click **Finish**. Wait until the format process completes. The secure hard drive will be recognized and it will be ready for use.

For the Windows 8 or Windows 8.1 operating system:

- 1. After a complete reset, connect the secure hard drive to your computer.
- 2. Input the default user password 12345678, and then press ildot to enter user mode. The operating system automatically installs all the USB device drivers for the secure hard drive.
- 3. From the desktop screen, right-click anywhere on the desktop, and then click **Personalize**. The Personalization window is displayed.
- 4. Click Change desktop icons in the top-left area.
- 5. Select **Computer**, and then click **OK**. The Computer icon is displayed on the desktop screen.
- 6. Right-click **Computer** on the desktop, and then click **Manage**. The Computer Management window opens.
- 7. Select **Disk Management**. The Initialize Disk windows opens.
- 8. Click MBR(Master Boot Record)OK.
- 9. Right-click your mouse in the blank area of the unallocated device section, and then select **New Simple Volume**.
- 10. Click **OK** → **OK** → **OK** → **Finish** with default settings. Wait until the format process completes. The secure hard drive will be recognized and it will be ready for use.

Chapter 4. Troubleshooting

This chapter contains troubleshooting information for the secure hard drive. If you encounter any of the following problems when using the secure hard drive, refer to the corresponding answers.

Q: Why could I not enter user mode after I connect the secure hard drive to the computer and input the correct user password?

A: The secure hard drive needs several seconds to be ready for password input. To solve the problem, wait for several seconds after you connect the secure hard drive to the computer, and then input your user password.

Q: What can I do if I forget the user password?

A: You can create a user password. To create a user password, do the following:

- 1. Enter administrator mode. See "Entering administrator mode" on page 5 for more information.
- 2. Delete all user passwords. See "Deleting the user password(s)" on page 8 for more information.
- 3. Create your new user password. See "Adding a new user password" on page 7 for more information.

Q: What can I do if I forget the administrator password?

A: There is no other way to retrieve the administrator password except a complete reset of the secure hard drive. After a complete reset, all data will be lost and you need to manually initialize and format the secure hard drive. Then you will be able to use the default administrator password 12345678. For more information, see "Completely resetting the secure hard drive" on page 9 and "Initializing and formatting the secure hard drive after a complete reset" on page 9.

Q: Why does the operating system not recognize the secure hard drive after I completely reset it and enter user mode?

A: You need to manually initialize and format the secure hard drive before you can use it. For more information, refer to "Initializing and formatting the secure hard drive after a complete reset" on page 9.

Q: Can I initialize and format the secure hard drive with a Windows user account?

A: No, this is a limitation of the Windows operating systems. You should use the Windows administrator account to initialize and format the secure hard drive.

Q: How do I use the secure hard drive without a password?

A: As a full disk encryption product, the secure hard drive can never be used without a password.

Q: What encryption algorithm is used in this product?

A: The secure hard drive uses the Advanced Encryption Standard (AES) 256-bit algorithm.

Q: Why could I not initialize, partition, or format the secure hard drive?

A: Ensure that you have administrator privileges. You can use only the Windows administrator account to initialize, partition, or format the secure hard drive in administrator mode.

Q: Why could the operating system not be started from the secure hard drive?

A: As this is a secure hard drive, before you use it, you will need several seconds to input a password and unlock the secure hard drive. When the secure hard drive is unlocked, the operating system has already finished the startup process.

Appendix A. Service and Support

The following information describes the technical support that is available for your product, during the warranty period or throughout the life of your product. Refer to the Lenovo Limited Warranty for a full explanation of Lenovo warranty terms.

Online technical support

Online technical support is available during the lifetime of a product at: http://support.lenovo.com

Product replacement assistance or exchange of defective components also is available during the warranty period. In addition, if your option is installed in a Lenovo computer, you might be entitled to service at your location. A Lenovo technical support representative can help you determine the best alternative.

Telephone technical support

Installation and configuration support through the Customer Support Center will be available until 90 days after the option has been withdrawn from marketing. After that time, the support is cancelled, or made available for a fee, at Lenovo's discretion. Additional support is also available for a nominal fee.

Before contacting a Lenovo technical support representative, please have the following information available: option name and number, proof of purchase, computer manufacturer, model, serial number and manual, the exact wording of any error message, description of the problem, and the hardware and software configuration information for your system.

Your technical support representative might want to walk you through the problem while you are at your computer during the call.

Telephone numbers are subject to change without notice. The most up-to-date telephone list for Lenovo Support is always available at <u>http://www.lenovo.com/support/phone</u>. If the telephone number for your country or region is not listed, contact your Lenovo reseller or Lenovo marketing representative.

Appendix B. Lenovo Limited Warranty

L505-0010-02 08/2011

This Lenovo Limited Warranty consists of the following parts:

Part 1 - General Terms

Part 2 - Country-specific Terms

Part 3 - Warranty Service Information

The terms of Part 2 replace or modify terms of Part 1 as specified for a particular country.

Part 1 - General Terms

This Lenovo Limited Warranty applies only to Lenovo hardware products you purchased for your own use and not for resale. This Lenovo Limited Warranty is available in other languages at www.lenovo.com/warranty.

What this Warranty Covers

Lenovo warrants that each Lenovo hardware product that you purchase is free from defects in materials and workmanship under normal use during the warranty period. The warranty period for the product starts on the original date of purchase as shown on your sales receipt or invoice or as may be otherwise specified by Lenovo. The warranty period and type of warranty service that apply to your product are as specified in "**Part 3 - Warranty Service Information**" below. This warranty only applies to products in the country or region of purchase.

THIS WARRANTY IS YOUR EXCLUSIVE WARRANTY AND REPLACES ALL OTHER WARRANTIES OR CONDITIONS, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, ANY IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. AS SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF EXPRESS OR IMPLIED WARRANTIES, THE ABOVE EXCLUSION MAY NOT APPLY TO YOU. IN THAT EVENT, SUCH WARRANTIES APPLY ONLY TO THE EXTENT AND FOR SUCH DURATION AS REQUIRED BY LAW AND ARE LIMITED IN DURATION TO THE WARRANTY PERIOD. AS SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON THE DURATION OF AN IMPLIED WARRANTY, THE ABOVE LIMITATION ON DURATION MAY NOT APPLY TO YOU.

How to Obtain Warranty Service

If the product does not function as warranted during the warranty period, you may obtain warranty service by contacting Lenovo or a Lenovo approved Service Provider. A list of approved Service Providers and their telephone numbers is available at: www.lenovo.com/support/phone.

Warranty service may not be available in all locations and may differ from location to location. Charges may apply outside a Service Provider's normal service area. Contact a local Service Provider for information specific to your location.

Customer Responsibilities for Warranty Service

Before warranty service is provided, you must take the following steps:

• follow the service request procedures specified by the Service Provider;

- backup or secure all programs and data contained in the product;
- provide the Service Provider with all system keys or passwords;
- provide the Service Provider with sufficient, free, and safe access to your facilities to perform service;
- remove all data, including confidential information, proprietary information and personal information, from the product or, if you are unable to remove any such information, modify the information to prevent its access by another party or so that it is not personal data under applicable law. The Service Provider shall not be responsible for the loss or disclosure of any data, including confidential information, proprietary information, or personal information, on a product returned or accessed for warranty service;
- remove all features, parts, options, alterations, and attachments not covered by the warranty;
- ensure that the product or part is free of any legal restrictions that prevent its replacement;
- if you are not the owner of a product or part, obtain authorization from the owner for the Service Provider to provide warranty service.

What Your Service Provider Will Do to Correct Problems

When you contact a Service Provider, you must follow the specified problem determination and resolution procedures.

The Service Provider will attempt to diagnose and resolve your problem by telephone, e-mail or remote assistance. The Service Provider may direct you to download and install designated software updates.

Some problems may be resolved with a replacement part that you install yourself called a "Customer Replaceable Unit" or "CRU." If so, the Service Provider will ship the CRU to you for you to install.

If your problem cannot be resolved over the telephone; through the application of software updates or the installation of a CRU, the Service Provider will arrange for service under the type of warranty service designated for the product under "**Part 3 - Warranty Service Information**" below.

If the Service Provider determines that it is unable to repair your product, the Service Provider will replace it with one that is at least functionally equivalent.

If the Service Provider determines that it is unable to either repair or replace your product, your sole remedy under this Limited Warranty is to return the product to your place of purchase or to Lenovo for a refund of your purchase price.

Replacement Products and Parts

When warranty service involves the replacement of a product or part, the replaced product or part becomes Lenovo's property and the replacement product or part becomes your property. Only unaltered Lenovo products and parts are eligible for replacement. The replacement product or part provided by Lenovo may not be new, but it will be in good working order and at least functionally equivalent to the original product or part. The replacement product or the balance of the period remaining on the original product.

Use of Personal Contact Information

If you obtain service under this warranty, you authorize Lenovo to store, use and process information about your warranty service and your contact information, including name, phone numbers, address, and e-mail address. Lenovo may use this information to perform service under this warranty. We may contact you to inquire about your satisfaction with our warranty service or to notify you about any product recalls or safety issues. In accomplishing these purposes, you authorize Lenovo to transfer your information to any country where we do business and to provide it to entities acting on our behalf. We may also disclose it where required by law. Lenovo's privacy policy is available at www.lenovo.com/.

What this Warranty Does not Cover

This warranty does not cover the following:

- uninterrupted or error-free operation of a product;
- loss of, or damage to, your data by a product;
- any software programs, whether provided with the product or installed subsequently;
- failure or damage resulting from misuse, abuse, accident, modification, unsuitable physical or operating environment, natural disasters, power surges, improper maintenance, or use not in accordance with product information materials;
- damage caused by a non-authorized service provider;
- failure of, or damage caused by, any third party products, including those that Lenovo may provide or integrate into the Lenovo product at your request;
- any technical or other support, such as assistance with "how-to" questions and those regarding product set-up and installation;
- products or parts with an altered identification label or from which the identification label has been removed.

Limitation of Liability

Lenovo is responsible for loss or damage to your product only while it is in the Service Provider's possession or in transit, if the Service Provider is responsible for the transportation.

Neither Lenovo nor the Service Provider is responsible for loss or disclosure of any data, including confidential information, proprietary information, or personal information, contained in a product.

UNDER NO CIRCUMSTANCES, AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SET FORTH HEREIN, SHALL LENOVO, ITS AFFILIATES, SUPPLIERS, RESELLERS, OR SERVICE PROVIDERS BE LIABLE FOR ANY OF THE FOLLOWING EVEN IF INFORMED OF THEIR POSSIBILITY AND REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY OF LIABILITY: 1) THIRD PARTY CLAIMS AGAINST YOU FOR DAMAGES; 2) LOSS, DAMAGE OR DISCLOSURE OF YOUR DATA; 3) SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOST PROFITS, BUSINESS REVENUE, GOODWILL OR ANTICIPATED SAVINGS. IN NO CASE SHALL THE TOTAL LIABILITY OF LENOVO, ITS AFFILIATESS, SUPPLIERS, RESELLERS OR SERVICE PROVIDERS FOR DAMAGES FROM ANY CAUSE EXCEED THE AMOUNT OF ACTUAL DIRECT DAMAGES, NOT TO EXCEED THE AMOUNT PAID FOR THE PRODUCT.

THE FOREGOING LIMITATIONS DO NOT APPLY TO DAMAGES FOR BODILY INJURY (INCLUDING DEATH), DAMAGE TO REAL PROPERTY OR DAMAGE TO TANGIBLE PERSONAL PROPERTY FOR WHICH LENOVO IS LIABLE UNDER LAW. AS SOME STATES OR JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

Your Other Rights

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS ACCORDING TO THE APPLICABLE LAWS OF YOUR STATE OR JURISDICTION. YOU MAY ALSO HAVE OTHER RIGHTS UNDER A WRITTEN AGREEMENT WITH LENOVO. NOTHING IN THIS WARRANTY AFFECTS STATUTORY RIGHTS, INCLUDING RIGHTS OF CONSUMERS UNDER LAWS OR REGULATIONS GOVERNING THE SALE OF CONSUMER GOODS THAT CANNOT BE WAIVED OR LIMITED BY CONTRACT.

Part 2 - Country-specific Terms

Australia

"Lenovo" means Lenovo (Australia & New Zealand) Pty Limited ABN 70 112 394 411. Address: Level 10, North Tower, 1-5 Railway Street, Chatswood, NSW, 2067. Telephone: +61 2 8003 8200. Email: lensyd_au@lenovo.com

The following replaces the same section in Part 1:

What this Warranty Covers:

Lenovo warrants that each hardware product that you purchase is free from defects in materials and workmanship under normal use and conditions during the warranty period. If the product fails due to a covered defect during the warranty period, Lenovo will provide you a remedy under this Limited Warranty. The warranty period for the product starts on the original date of purchase specified on your sales receipt or invoice unless Lenovo informs you otherwise in writing. The warranty period and type of warranty service that apply to your product are set forth below in **Part 3 - Warranty Service Information**.

THE BENEFITS GIVEN BY THIS WARRANTY ARE IN ADDITION TO YOUR RIGHTS AND REMEDIES AT LAW, INCLUDING THOSE UNDER THE AUSTRALIAN CONSUMER LAW.

The following replaces the same section in Part 1:

Replacement Products and Parts:

When warranty service involves the replacement of a product or part, the replaced product or part becomes Lenovo's property and the replacement product or part becomes your property. Only unaltered Lenovo products and parts are eligible for replacement. The replacement product or part provided by Lenovo may not be new, but it will be in good working order and at least functionally equivalent to the original product or part. The replacement product or part shall be warranted for the balance of the period remaining on the original product. Products and parts presented for repair may be replaced by refurbished products or parts of the same type rather than being repaired. Refurbished parts may be used to repair the product; and repair of the product may result in loss of data, if the product is capable of retaining user-generated data.

The following is added to the same section in Part 1:

Use of Personal Contact Information:

Lenovo will not be able to perform our service under this warranty if you refuse to provide your information or do not wish us to transfer your information to our agent or contractor. You have the right to access your personal contact information and request correction of any errors in it pursuant to the Privacy Act 1988 by contacting Lenovo.

The following replaces the same section in Part 1:

Limitation of Liability:

Lenovo is responsible for loss or damage to your product only while it is in the Service Provider's possession or in transit, if the Service Provider is responsible for the transportation.

Neither Lenovo nor the Service Provider is responsible for loss or disclosure of any data, including confidential information, proprietary information, or personal information, contained in a product.

TO THE EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES AND NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY REMEDY SET FORTH HEREIN, SHALL LENOVO, ITS AFFILIATES, SUPPLIERS, RESELLERS, OR SERVICE PROVIDERS BE LIABLE FOR ANY OF THE FOLLOWING EVEN IF INFORMED OF THEIR POSSIBILITY AND REGARDLESS OF WHETHER THE CLAIM IS BASED IN CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER THEORY OF LIABILITY: 1) THIRD PARTY CLAIMS AGAINST YOU FOR DAMAGES; 2) LOSS, DAMAGE OR DISCLOSURE OF YOUR DATA; 3) SPECIAL, INCIDENTAL, PUNITIVE, INDIRECT OR CONSEQUENTIAL DAMAGES, INCLUDING BUT NOT LIMITED TO LOST PROFITS, BUSINESS REVENUE, GOODWILL OR ANTICIPATED SAVINGS. IN NO CASE SHALL THE TOTAL LIABILITY OF LENOVO, ITS AFFILIATESS, SUPPLIERS, RESELLERS OR SERVICE PROVIDERS FOR DAMAGES FROM ANY CAUSE EXCEED THE AMOUNT OF ACTUAL DIRECT DAMAGES, NOT TO EXCEED THE AMOUNT PAID FOR THE PRODUCT.

THE FOREGOING LIMITATIONS DO NOT APPLY TO DAMAGES FOR BODILY INJURY (INCLUDING DEATH), DAMAGE TO REAL PROPERTY OR DAMAGE TO TANGIBLE PERSONAL PROPERTY FOR WHICH LENOVO IS LIABLE UNDER LAW.

The following replaces the same section in Part 1:

Your Other Rights:

THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU ALSO HAVE OTHER RIGHTS AT LAW, INCLUDING UNDER THE AUSTRALIAN CONSUMER LAW. NOTHING IN THIS WARRANTY AFFECTS STATUTORY RIGHTS OR RIGHTS AT LAW, INCLUDING RIGHTS THAT CANNOT BE WAIVED OR LIMITED BY CONTRACT.

For example, our products come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the products repaired or replaced if the products fail to be of acceptable quality and the failure does not amount to a major failure.

New Zealand

The following is added to the same section in Part 1:

Use of Personal Information:

Lenovo will not be able to perform our service under this warranty if you refuse to provide your information or do not wish us to transfer your information to our agent or contractor. You have the right to access your personal information and request correction of any errors in it pursuant to the Privacy Act 1993 by contacting Lenovo (Australia & New Zealand) Pty Limited ABN 70 112 394 411. Address: Level 10, North Tower, 1-5 Railway Street, Chatswood, NSW, 2067. Telephone: 61 2 8003 8200. Email: lensyd_au@lenovo.com

Bangladesh, Cambodia, India, Indonesia, Nepal, Philippines, Vietnam and Sri Lanka

The following is added to Part 1:

Dispute Resolution

Disputes arising out of or in connection with this warranty shall be finally settled by arbitration held in Singapore. This warranty shall be governed, construed and enforced in accordance with the laws of Singapore, without regard to conflict of laws. If you acquired the product in **India**, disputes arising out of or in connection with this warranty shall be finally settled by arbitration held in Bangalore, India. Arbitration in Singapore shall be held in accordance with the Arbitration Rules of Singapore International Arbitration Center ("SIAC Rules") then in effect. Arbitration in India shall be held in accordance with the laws of India then in effect. The arbitration award shall be final and binding on the parties without appeal. Any award shall be in writing and set forth the findings of fact and the conclusions of law. All arbitration proceedings, including all documents presented in such proceedings shall be conducted in the English language. The English language version of this warranty prevails over any other language version in such proceedings.

European Economic Area (EEA)

The following is added to Part 1:

Customers in the EEA may contact Lenovo at the following address: EMEA Service Organisation, Lenovo (International) B.V., Floor 2, Einsteinova 21, 851 01, Bratislava, Slovakia. Service under this warranty for Lenovo hardware products purchased in EEA countries may be obtained in any EEA country in which the product has been announced and made available by Lenovo.

Russia

The following is added to Part 1:

Product Service Life

The product service life is four (4) years from the original date of purchase.

Part 3 - Warranty Service Information

Product Type	Country or Region of Purchase	Warranty Period	Type of Warranty Service
ThinkPad USB 3.0 Secure Hard Drive	Worldwide	3 years	1, 4

If required, your Service Provider will provide repair or exchange service depending on the type of warranty service specified for your product and the available service. Scheduling of service will depend upon the time of your call, parts availability, and other factors.

Types of Warranty Service

1. Customer Replaceable Unit ("CRU") Service

Under CRU Service, the Service Provider will ship CRUs to you at its cost for installation by you. CRU information and replacement instructions are shipped with your product and are available from Lenovo at any time upon request. CRUs that are easily installed by you are called "Self-service CRUs". "Optional-service CRUs" are CRUs that may require some technical skill and tools. Installation of Self-service CRUs is your responsibility. You may request that a Service Provider install Optional-service CRUs under one of the other types of warranty service designated for your product. An optional service CRUs would be installed for you. You may find a list of CRUs and their designation in the publication that was shipped with your product or at www.lenovo.com/CRUs. The requirement to return a defective CRU, if any, will be specified in the instructions shipped with a replacement CRU. When return is required: 1) return instructions, a prepaid for the replacement CRU if the Service Provider does not receive the defective CRU from you within thirty (30) days of your receipt of the replacement CRU.

2. On-site Service

Under On-Site Service, a Service Provider will either repair or exchange the product at your location. You must provide a suitable working area to allow disassembly and reassembly of the product. Some repairs may need to be completed at a service center. If so, the Service Provider will send the product to the service center at its expense.

3. Courier or Depot Service

Under Courier or Depot Service, your product will be repaired or exchanged at a designated service center, with shipping at the expense of the Service Provider. You are responsible for disconnecting the product and packing it in a shipping container provided to you to return your product to a designated service center. A courier will pick up your product and deliver it to the designated service center. The service center will return the product to you at its expense.

4. Customer Carry-In Service

Under Customer Carry-In Service, your product will be repaired or exchanged after you deliver it to a designated service center at your risk and expense. After the product has been repaired or exchanged, it will be made available to you for collection. If you fail to collect the product, the Service Provider may dispose of the product as it sees fit, with no liability to you.

5. Mail-In Service

Under Mail-In Service, your product will be repaired or exchanged at a designated service center after you deliver it at your risk and expense. After the product has been repaired or exchanged, it will be returned to you at Lenovo's risk and expense, unless the Service Provider specifies otherwise.

6. Customer Two-Way Mail-In Service

Under Customer Two-Way Mail-In Service, your product will be repaired or exchanged after you deliver it to a designated service center at your risk and expense. After the product has been repaired or exchanged, it will be made available to you for return shipping at your risk and expense. If you fail to arrange return shippent, the Service Provider may dispose of the product as it sees fit, with no liability to you.

7. Product Exchange Service

Under Product Exchange Service, Lenovo will ship a replacement product to your location. You are responsible for its installation and verification of its operation. The replacement product becomes your property in exchange for the failed product, which becomes the property of Lenovo. You must pack the failed product in the shipping carton in which you received the replacement product and return it to Lenovo. Transportation charges, both ways, shall be at Lenovo's expense. If you fail to use the carton in which the replacement product was received, you may be responsible for any damage to the failed product occurring during shipment. You may be charged for the replacement product if Lenovo does not receive the failed product within thirty (30) days of your receipt of the replacement product.

Suplemento de Garantía para México

Este Suplemento se considera parte integrante de la Garantía Limitada de Lenovo y será efectivo única y exclusivamente para los productos distribuidos y comercializados dentro del Territorio de los Estados Unidos Mexicanos. En caso de conflicto, se aplicarán los términos de este Suplemento.

Todos los programas de software precargados en el equipo sólo tendrán una garantía de treinta (30) días por defectos de instalación desde la fecha de compra. Lenovo no es responsable de la información incluida en dichos programas de software y/o cualquier programa de software adicional instalado por Usted o instalado después de la compra del producto.

Los servicios no cubiertos por la garantía se cargarán al usuario final, previa obtención de una autorización.

En el caso de que se precise una reparación cubierta por la garantía, por favor, llame al Centro de soporte al cliente al 001-866-434-2080, donde le dirigirán al Centro de servicio autorizado más cercano. Si no existiese ningún Centro de servicio autorizado en su ciudad, población o en un radio de 70 kilómetros

de su ciudad o población, la garantía incluirá cualquier gasto de entrega razonable relacionado con el transporte del producto a su Centro de servicio autorizado más cercano. Por favor, llame al Centro de servicio autorizado más cercano para obtener las aprobaciones necesarias o la información relacionada con el envío del producto y la dirección de envío.

Para obtener una lista de los Centros de servicio autorizados, por favor, visite: http://www.lenovo.com/mx/es/servicios

Importado por: Lenovo México S. de R.L. de C.V. Av. Santa Fe 505, Piso 15 Col. Cruz Manca Cuajimalpa, D.F., México C.P. 05349 Tel. (55) 5000 8500

Appendix C. Electronic emission notices

The following information refers to the ThinkPad USB 3.0 Secure Hard Drive.

Federal Communications Commission Declaration of Conformity

ThinkPad USB 3.0 Secure Hard Drive - 0A65616, 0A65619

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an authorized dealer or service representative for help.

Lenovo is not responsible for any radio or television interference caused by using other than specified or recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party: Lenovo (United States) Incorporated 1009 Think Place - Building One Morrisville, NC 27560 Phone Number: 919-294-5900



Industry Canada Class B emission compliance statement

This Class B digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

European Union - Compliance to the Electromagnetic Compatibility Directive

This product is in conformity with the protection requirements of EU Council Directive 2004/108/EC on the approximation of the laws of the Member States relating to electromagnetic compatibility. Lenovo cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the installation of option cards from other manufacturers.

This product has been tested and found to comply with the limits for Class B Information Technology Equipment according to European Standard EN 55022. The limits for Class B equipment were derived for typical residential environments to provide reasonable protection against interference with licensed communication devices.

Lenovo, Einsteinova 21, 851 01 Bratislava, Slovakia

CE

German Class B compliance statement

Deutschsprachiger EU Hinweis:

Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der Lenovo empfohlene Kabel angeschlossen werden. Lenovo übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der Lenovo verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der Lenovo gesteckt/eingebaut werden.

Deutschland:

Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Betriebsmitteln Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln" EMVG (früher "Gesetz über die elektromagnetische Verträglichkeit von Geräten"). Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG (früher 89/336/EWG) in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Betriebsmitteln, EMVG vom 20. Juli 2007 (früher Gesetz über die elektromagnetische Verträglichkeit von Geräten), bzw. der EMV EG Richtlinie 2004/108/EC (früher 89/336/EWG), für Geräte der Klasse B.

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen. Verantwortlich für die Konformitätserklärung nach Paragraf 5 des EMVG ist die Lenovo (Deutschland) GmbH, Gropiusplatz 10, D-70563 Stuttgart.

Informationen in Hinsicht EMVG Paragraf 4 Abs. (1) 4: Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse B.

Korea Class B compliance statement

B급 기기(가정용 방송통신기자재)
이 기기는 가정용(B급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며, 모든 지역에서 사용할 수 있습니다

Japan VCCI Class B compliance statement

```
この装置は、クラスB情報技術装置です。 この装置は、家庭環境で使用するこ
とを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使
用されると、受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI-B
```

Lenovo product service information for Taiwan

台灣 Lenovo 産品服務資訊如下: 荷蘭商聯想股份有限公司台灣分公司 台北市信義區信義路五段七號十九樓之一 服務電話:0800-000-702

Ukraine Compliance Mark

001

Eurasian compliance mark



Appendix D. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc. 1009 Think Place - Building One Morrisville, NC 27560 U.S.A. Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Recycling information

Lenovo encourages owners of information technology (IT) equipment to responsibly recycle their equipment when it is no longer needed. Lenovo offers a variety of programs and services to assist equipment owners in recycling their IT products. For information on recycling Lenovo products, go to: http://www.lenovo.com/recycling

Recycling and disposal information for Japan is available at: http://www.lenovo.com/recycling/japan

Recycling information for Brazil

Declarações de Reciclagem no Brasil

Descarte de um Produto Lenovo Fora de Uso

Equipamentos elétricos e eletrônicos não devem ser descartados em lixo comum, mas enviados à pontos de coleta, autorizados pelo fabricante do produto para que sejam encaminhados e processados por empresas especializadas no manuseio de resíduos industriais, devidamente certificadas pelos orgãos ambientais, de acordo com a legislação local.

A Lenovo possui um canal específico para auxiliá-lo no descarte desses produtos. Caso você possua um produto Lenovo em situação de descarte, ligue para o nosso SAC ou encaminhe um e-mail para: reciclar@lenovo.com, informando o modelo, número de série e cidade, a fim de enviarmos as instruções para o correto descarte do seu produto Lenovo.

Export Classification Notice

This product is subject to the United States Export Administration regulations (EAR) and has an Export Classification Control Number (ECCN) of 5A992.c. It can be re-exported except to any of the embargoed countries in the EAR E1 country list.

Trademarks

Lenovo and ThinkPad are trademarks of Lenovo in the United States, other countries, or both.

Windows is a trademark of the Microsoft group of companies.

Other company, product, or service names may be trademarks or service marks of others.

Appendix E. Restriction of Hazardous Substances Directive (RoHS)

European Union RoHS

Lenovo products sold in the European Union, on or after 3 January 2013 meet the requirements of Directive 2011/65/EU on the restriction of the use of certain hazardous substances in electrical and electronic equipment ("RoHS recast" or "RoHS 2").

For more information about Lenovo progress on RoHS, go to: http://www.lenovo.com/social_responsibility/us/en/RoHS_Communication.pdf

China RoHS

The information in the following table is applicable for products manufactured on or after March 1, 2007 for sale in the People's Republic of China.

	有毒有害物质或元素					
Lenovo 电脑选件	铅 (Pb)	汞 (Hg)	镉 (Cd)	六价铬 (Cr(VI))	多溴联苯 (PBB)	多溴二苯醚 (PBDE)
硬盘驱动器	x	0	0	0	Ο	0
 ○:表示该有毒有害物质在该部件所有均质材料中的含量均在SJ/T 11363-2006标准 规定的限量要求以下。 X:表示该有毒有害物质至少在该部件的某一均质材料中的含量超出SJ/T 11363-2006标准规定的限量要求。 对于销往欧盟的产品,标有"X"的项目均符合欧盟指令2002/95/EC 豁免条款。 ④ 在中华人民共和国境内销售的电子信息产品上将印有"环保使用期" (EPuP)符号。圆圈中的数字代表产品的正常环保使用年限。 						

Turkish RoHS

The Lenovo product meets the requirements of the Republic of Turkey Directive on the Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment (EEE).

Türkiye EEE Yönetmeliğine Uygunluk Beyanı

Bu Lenovo ürünü, T.C. Çevre ve Orman Bakanlığı'nın "Elektrik ve Elektronik Eşyalarda Bazı Zararlı Maddelerin Kullanımının Sınırlandırılmasına Dair Yönetmelik (EEE)" direktiflerine uygundur.

EEE Yönetmeliğine Uygundur.

Ukraine RoHS

Цим підтверджуємо, що продукція Леново відповідає вимогам нормативних актів України, які обмежують вміст небезпечних речовин

India RoHS

RoHS compliant as per E-Waste (Management & Handling) Rules, 2011.

ThinkPad.