KEY™ SECUREPC

KEYSECUREPC

GENERAL OPERATING PRINCIPLES

IMPORTANT: BEFORE STARTING KEYSECUREPC ON YOUR COMPUTER, PLEASE READ THIS MANUAL CAREFULLY.

MORE PARTICULARLY, PLEASE READ THE SECTIONS RELATED TO:

- THE 3 REQUIRED PASSWORDS
- THE 2 WORK ENVIRONMENTS
- WIPING (DELIBERATE DATA DELETION)

PLEASE READ CAREFULLY!
THESE SECTIONS CONTAIN ESSENTIAL INFORMATION FOR THE PROPER USE OF KEYSECUREPC AND THE SAFETY OF YOUR DATA!

EMA060511_UK

KEY™ SECUREPC

INDEX

GENERAL KEYSECUREPC OPERATING PRINCIPLES.

These initial pages describe the KeySecurePC system's general operating principles.
This description is meant to be brief and non-technical, thereby allowing even a novice to understand the general operating principles of KeySecurePC. Please visit our website www.keysecurepc.com if you would like information of a more technical nature.

KeySecurePC is not an ordinary encrypted USB drive or external memory storage.
Unlike standard encrypted USB drives, it contains its own internal operating system, programmes, and space for storing data.

It works very simply. When connected to a computer, KeySecurePC:

- replaces the hard drive, operating system and programmes of the host computer;
- redirects all data management to itself using its internal operating system and programmes.

By redirecting data management to itself, KeySecurePC prevents the computer from creating and saving data of any type, including temporary files, links, histories, or any trace of your activities, which would otherwise remain hidden for years in your PC's hard disk, operating system and programmes and could be recovered by anyone at any time using data recovery software.

No traditional system offers such complete security for the computer on which you work:

- no encrypted USB drive;
- no data protection software;
- no encrypted hardware.

All these systems have the same weakness: when they hide or delete your files, they only hide or delete the visible copies of the files you work on and do not remove the so-called "temporary files", links, and histories, or copies of your data that the computer continuously and automatically creates and saves on the hard disk, in the operating system, and in programmes.

Temporary files, contrary to their name, are saved for years by your computer. They are "ghost" files that remain hidden for years in the memory of your computer, keeping track of your Internet surfing and the files that you manage or download. Recovering this data is very easy. All that is needed is a data recovery programme to recover and generate an exact copy of what you thought you had deleted forever.

That is why it is no use:

- deleting files;
- moving them to an external memory;
- saving them on an encrypted USB drive;
- formatting your hard drive, even over and over again.

All these actions remove, conceal or delete the visible copy of files, but do not remove temporary files, histories or links, which remain hidden for years on the hard disk, in the operating system, and in programmes on your computer, ready to be retrieved by a data recovery program.

WITH KEYSECUREPC YOU CAN USE YOUR PC AND NO TRACE OF YOUR WORK SESSION REMAINS ON YOUR COMPUTER.

No trace remains:

- of your web history;
- of files used or downloaded;
- of emails exchanged;
- of video, music, pictures.

All your data is internally saved on KeySecurePC where it is protected by full AES256 encryption. AES stands for "Advanced Encryption Standard", and is an encryption algorithm that has never been broken and is considered unbreakable with the computing power of current computers.

Not surprisingly, AES256 encryption ensures a safety level equal to that presently used by the intelligence agencies of many countries to protect their Top Secret documents.

In considering the level of security offered by KeySecurePC, bear in mind that KeySecurePC does not encrypt individual files, as encrypted USB drives often do, but actually encrypts THE ENTIRE OPERATING SYSTEM and, consequently, all programmes and every piece of data therein.

It is impossible for anyone to access a single file unless they know your password; they would have to override the entire system, which is impossible given the level of security presently guaranteed by full AES256 encryption.

KeySecurePC is one of the few systems in the world with built-in "Wiping", an option for the deliberate and irreversible deletion of data.

This feature may seem excessive, but many professionals and entrepreneurs appreciate having, in extreme cases, the option of destroying data rather than letting it fall into the wrong hands.

With regard to this aspect, it is important to remember that Wiping involves repeated overwriting of random and illegible data on the same sectors containing the original files.
Just minutes after implementation, the KeySecurePC Wiping function overwrites every single piece of data stored therein and thereby increases the protection and security offered by KeySecurePC.

THE DUAL KEYSECUREPC ENVIRONMENT.

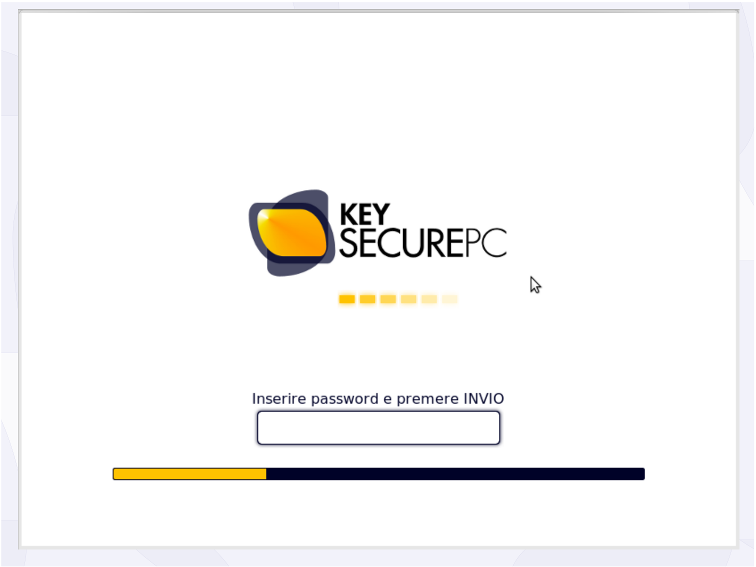
We all know that a personal computer provides several work environments, or in other words, that it may be operated by different users with different passwords. If, for example, you share your computer with your wife, every time you turn on the computer you are asked to indicate which user environment you want to access, and after you have chosen one, the computer asks for the password. Each individual computer can have a very large number of users/environments.

KeySecurePC – being a highly personal device – limits the number of environments to two.

The first environment has a limited storage capacity (1 GB on all KeySecurePC models) and is normally used to manage and store files that are considered less sensitive and/or are shared with other people like friends, family, or trusted co-workers. In order to access this environment, users must enter the 1st password (see the User Manual, which you can download from the download section on our website, www.keysecurepc.com).

The second environment has a far greater storage capacity (approximately 3 to 252 GB, depending on the KeySecurePC model chosen) and was designed for the personal and exclusive use of the KeySecurePC owner. In order to access this environment, users must type the 2nd password (see User Manual).

N.B.: For security reasons, the existence of the dual environment is not visible to anyone and access to the two environments is governed solely by password.
This means that when you run KeySecurePC on your computer, there is NO screen providing a choice between two different environments or users, as is common on PCs.
All that appears is a simple screen with password prompt like the one you see below. You decide whether to type the first, second, or third password, thus accessing the first or second environment (or, with the third password, wiping data).



Inserire password e premere INVIO

THE 3 PASSWORDS.

3.1
Data theft and brute force programmes: why it is important to carefully choose and protect your passwords.

No matter how obvious it may sound, the easiest way to enter a well-protected system is knowing the password. So for a data thief, it is much simpler to "steal" a password than try to crack a secure system: in fact, most cases of data theft occur further to discovery of a confidential password.

This simple concern is even more important considering that most data thefts are carried out by those closest to us (family, friends, colleagues) and who know us best; in other words, people who are more likely to know our password, perhaps by simply guessing it. This can happen because many of us choose passwords that are simple or related to our lives, because they are easier to remember. For example, some choose the name of their dog (FIDO), or their children (ANTHONY), or their date of birth (NewYork07031968). These passwords are easy to remember, but also easy to guess for those close to you.

Furthermore, the systems most commonly used by hackers to discover your password (so-called Brute Force programmes) are based on the programme's ability to gain access to the system by entering thousands of different passwords every minute, until it guesses the right one.
The first words that these programs try to use are those most common or otherwise present in the dictionary, such as first names or simple words like DOLL or CAR. Once all dictionary words are tried, the program tries random combinations of letters, created using the 26 letters of the keyboard, such as MALETHVS. The possible combinations it can try are endless and one can run a brute force programme for a very long time. In order to make it more difficult for a brute force programme, we can add numbers from the keyboard and create combinations such as M4N2K3LKJUIO645. Finally, letters and numbers can be combined with special characters like @ or $, or even punctuation characters.

If you add up the letters, numbers, and special characters on our keyboard, you will see that there is a very high number of possible combinations: so, if you create a password over 8 characters long with letters, numbers, and special characters arranged randomly, guessing your password will be very unlikely from a statistical point of view: even a brute force programme would have a difficult time!

So the security of a password depends on both its length and complexity, or the combination, in a random and unpredictable sequence, of letters, numbers, and special characters. You must be thinking: but how do I remember a password like KEFHU987@uh&61? Not to mention the fact that I need to remember three different ones, as required by KeySecurePC? Well, that does present some difficulty. Thankfully there are various tricks you can use to remember. We describe some in the next section.

3.2
How to create a secure password that is easy to remember.

This section describes some methods for creating and keeping a secure password.

A widely used method is as follows: Think of a poem or a saying that you know by heart: YOU CAN'T TEACH AN OLD DOG NEW TRICKS.

Your password can be created using the first letter of each word in the saying: YCTAODNT. This sequence of letters is easy to remember (just recite the saying ...) but virtually impossible for anyone else to identify.
In order to make your password even safer, add an @ at the beginning and a number at the end related to something easy to remember, for example the shirt number of your favourite player, and you have a crack-proof password: @YCTAODNT66.

If a poem or a saying still seems too popular, think of a notable phrase from your life that only you would know...in my case, for example, an old professor used to say "IF YOU DON'T STUDY YOU'LL ALL END UP DITCH DIGGERS", or IYDSYAEUDD, an excellent base for a strong password.

Other methods used include inversion of words. If it is easy for you to remember the words HOUSE and BOAT, combine and jumble them: houseboat becomes OHTUEOSBA, a random sequence of letters that can be made more secure by adding a number and repeating it the same number of times as the number itself (if it was five you should repeat it five times), perhaps with an @ dividing the letters and number. Your password becomes OHTUEOSBA@55555, easy for you to remember but impossible for anyone else to reconstruct.

There are also many websites on the internet that suggest ways to build a secure password: visit them to find other ideas and easily create your three KeySecurePC passwords. Remember that it is important to spend a few extra minutes on this activity now, because once you choose your KeySecurePC passwords, for security reasons, they cannot be changed without re-initializing the entire system!

After choosing your passwords, remember that their security depends on proper protection.
Remember:

- never tell anyone your password;
- never type the password in front of others;
- never write passwords on paper;
- never save them on your PC.

If you really want to keep track of your password be creative ... if your password is OHTUEOSBA@55555, keep photos of a house, a boat, and a player with the number 5...

3.3
The KeySecurePC passwords: it is important to choose them carefully, because they cannot be changed.

You must enter three different passwords into the system to use your KeySecurePC.

- The first password allows access to the system’s first environment;
- The second password allows access to the system’s second environment;
- The third password starts the wiping process – the deliberate destruction of data.

The three passwords are an integral part of KeySecurePC’s security technology.
Once entered into the system, they are encrypted and influence the AES256 encryption algorithm making it even more secure. For this reason, it is important to choose them carefully, following the suggestions found in the previous sections.
It is also IMPORTANT TO REMEMBER THAT THE THREE PASSWORDS CAN NOT BE CHANGED WITHOUT RE-INITIALIZING THE ENTIRE SYSTEM*. The reason for this is simple. As the passwords directly affect the encryption, any change could open a security vulnerability on the device, making it susceptible to attack.

* Re-initialization of the system involves the loss of all data stored on your KeySecurePC.
Anyone wishing to change their passwords can, but must first move all data to a backup device (for example our KeySecurePC Backup) and then re-copy it to the re-initialized system.