

Norman Privacy 3.0

Completely protect your private information!

Why use Privacy? There are many reasons why you should protect your information. For example, if you use the Internet or e-mail, your private correspondence is available to anyone who knows how to read it. This might be fine for ordinary messages, but not if they contain special text or file that you want only the recipient to read. Perhaps you have a notebook you carry around that contains confidential data. What if the hard disk 'fell' into the wrong hands? How would your organization suffer if the data were 'discovered' by your competitors? If you have any reason to be concerned about the privacy of your information

- in an e-mail,
 - on a removable disk, or
 - in a directory or file,
- then Privacy is the right solution for you.

What is Privacy?

Norman Privacy is data encryption and decryption software.

What is encryption and decryption?

Encryption changes data so that it is meaningless to anyone who does not have a key to unscramble it. For example, 'Hello' might be changed to "2kdi&k4". After you encrypt data, only you and the people you choose can decrypt (unscramble) the information to make it readable again. Privacy uses keys to ensure that only the people you want to read it can read your encrypted data. You can create as many keys for as many different people as you like.

Features Summary

Encrypt and decrypt

- removable disks
- directories
- files
- text
- Encrypt e-mails, including attachments if required
- Create self-decrypting files, directories and disks

- Compress encrypted data
- Set expiry dates for encrypted data
- Choose from three algorithms
- Securely handle original files

Encrypting and decrypting e-mails

When you send someone an e-mail, chances are that you don't want anyone else to read it. In fact, sometimes it is imperative that the intended recipient **and only** the intended recipient read it. But what if you accidentally type a wrong letter in the e-mail address? Or what if an unauthorized person opens someone else's e-mail program and reads the other person's e-mail?

And there are always 'hackers'; people who can tap into the computers that e-mail travels through. Hackers can intercept anyone's e-mail and read it. When you encrypt your e-mail, you can be sure it is read by only the person who has the key to decrypt it.

Encrypting e-mail

Privacy provides simple and flexible e-mail encryption. You can encrypt

- all of the contents of your e-mail, including attachments,

- just an attachment,
- just the message, or
- only parts of the message.

Decrypting e-mail

Decrypting e-mail that's been encrypted by Privacy is simple. If the whole e-mail including any attachments is encrypted, all you have to do is type the encryption key and everything automatically decrypts. You need Privacy installed to do this.

If only the attachment is encrypted, and it is encrypted as a self-decrypting file, you just double-click it and enter a key. You don't need Privacy installed to do this.

If just the message or part of the message is encrypted, use Privacy to decrypt it.

Self-decrypting files, directories, and disks

A self-decrypting file, directory, or disk is an encrypted file that you can decrypt without using any special software.

When creating a self-decrypting file, directory, or disk, Privacy compresses the information, then encrypts it to create an *Encrypted.exe* file.

To decrypt the *Encrypted.exe* file on any computer you don't need to have Privacy installed. All you have to do is double-click the *Encrypted.exe* file and enter the key. Simple!

Encryption compression

Whenever you encrypt information, you can set Privacy to automatically compress the information before it encrypts it.

When you encrypt a large amount of text in a document, for example, ten pages, compression decreases the number of encrypted pages required to store the text to, for example, five pages. When you encrypt any other

information (a file, directory, or removable disk), compression reduces the amount of disk space required to store the encrypted information.

Encryption expiry dates

When you encrypt information you can set an "encryption expiry date". This is the date on which you want the encrypted information to become inaccessible (so no one can decrypt it anymore).

About keys and how you organize them

Privacy uses the **key** together with the algorithm to encrypt and decrypt information. You can create as many different keys as you like.

When you want other people to decrypt your information, you tell them, in a manner suitably secure for your environment, the key you used to encrypt the information. They use that key to decrypt your information, and if necessary, encrypt information for you. Privacy lets you associate an **alias** to a key to make the key easier to remember. You can export aliases to people so they can use them to decrypt your information and encrypt information for you. The people who you export an alias to never know the actual key that is associated with the alias. To organize your aliases you can create **profiles**, which are groups of related aliases. Multiple users can use the one copy of Privacy, but each user cannot access the key details of any other user.

System requirements

You can install Privacy on any computer using an Intel compatible processor and running Windows . 95, Windows . 98, Windows . 2000, or Windows . NT version 4.x.