## [ This is WINGUARD.WRI, the WinGuard documentation file. ]

***PLEASE NOTE: FOR SECURITY PURPOSES, DO NOT COPY THIS FILE TO THE HARD DISK OF ANY COMPUTER TO BE PROTECTED BY WINGUARD, AS THIS FILE DISCUSSES WINGUARD FEATURES OF WHICH A GUEST USER SHOULD NOT BE AWARE !!!***

## WINGUARD.WRI CONTENTS



## PRODUCT LEGAL INFORMATION

**First, the necessary legal statements:**



**CETUS SOFTWARE AND FREDERICK WASTI DISCLAIM ALL WARRANTIES RELATING TO THIS SOFTWARE, WHETHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND ALL SUCH WARRANTIES ARE EXPRESSLY AND SPECIFICALLY DISCLAIMED.  NEITHER CETUS SOFTWARE NOR FREDERICK WASTI SHALL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, OR INCIDENTAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE SUCH SOFTWARE EVEN IF CETUS SOFTWARE OR FREDERICK WASTI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR CLAIMS.  IN NO EVENT SHALL THE LIABILITY OF CETUS SOFTWARE OR FREDERICK WASTI EVER EXCEED THE PRICE PAID FOR THE LICENSE TO USE THE SOFTWARE, REGARDLESS OF THE FORM OF THE CLAIM.  THE PERSON USING THE SOFTWARE BEARS ALL RISK AS TO THE QUALITY AND PERFORMANCE OF THE SOFTWARE.**

**This agreement shall be governed by the laws of the Commonwealth of Massachusetts and shall inure to the benefit of Cetus Software and/or Frederick Wasti, and any successors, administrators, heirs, and assigns.  Any action or proceeding brought by**

either party against the other arising out of or related to this agreement shall be brought only in a state or federal court of competent jurisdiction located in the Commonwealth of Massachusetts. The parties hereby consent to in personam jurisdiction of said courts.

This software and the disk on which it is obtained is licensed to an individual or institution user, for his/her/its own use. This is copyrighted software. The user is not obtaining title to the software or any copyright rights. The user may not sublicense, rent, lease, convey, modify, translate, convert to another programming language, decompile, or disassemble the software for any purpose. The user may make one copy of the software for back-up purposes only. The user may use this software on his/her/its own computer(s) only.

## OVERVIEW OF WINGUARD

WinGuard can protect a personal computer running Windows 3.1 from having any of its Program Manager groups or items rearranged or damaged (accidentally or intentionally). These protections would probably be most useful to someone in charge of a number of computers at a school or business, though a parent might wish to prevent little fingers on a mouse from dragging all of the Program Manager icons into a (not so) nice "happy face"!

WinGuard provides for the automatic setting of any one of seven different protection levels (actually, eight, including a "zero protection" setting), as well as allowing the hiding of "sensitive" programs, such as Windows Setup, Control Panel, or File Manager, behind its password-protected shell. WinGuard also allows the hiding of selected Program Manager groups and Control Panel icons, restricting access to them to the authorized user only.

Thus, it can be seen that WinGuard enables the authorized user to configure the Program Manager interface to allow the guest user easy access to selected applications, while minimizing the chances of damage (accidental or intentional) to Windows and the programs accessible through it.

## WHAT'S NEW IN VERSION 2

Version 2 of WinGuard has several features not present in Version 1:

1. V.2 lets you hide (and redisplay, of course) individual Program Manager groups. This might perhaps be the most useful of the new V.2 features. Besides allowing you to hide any of the regular groups of icons (such as Main, Accessories, Applications, etc.), it also gives you the chance to create a new hidden group just for your more "sensitive" icons: Create a brand new group, drag and drop the icons you wish to protect into it, and then hide it (and them) by using WinGuard V.2.

2. V.2, like V.1, allows you to remove from Program Manager many "sensitive" icons (such as the ones for File Manager, Control Panel, System Editor, PIF Editor, and Windows Setup), while still giving you access to them from within WinGuard. However, V.2 now provides convenient pushbuttons (as well as V.1-style menu items) for these Windows programs, thus making for quicker and easier access.

3. V.2 gives you the chance to hide (and redisplay) one or more of the icons that are in Control Panel's own window, without having to hide the main Control Panel icon, itself. (V.2 also has pushbuttons for each of the twelve regular Control Panel functions, giving you quick access to even the hidden icons, without the necessity of redisplaying them.)

4. V.2 allows you to prevent the guest user from exiting from Windows by any normal means (by using Program Manager's File Menu Exit Windows command or Control Menu

**Close command, or by double-clicking on the Control Menu Icon). (The authorized user may still exit from Windows from within WinGuard.)**

**5. V.2 lets you replace access to Task List (obtainable by double-clicking with the mouse on the desktop, or by using the Ctrl-Esc key combination) with quick access to WinGuard, instead. (WinGuard will still provide both pushbutton and menu access to Task List from within itself.) Furthermore, if you are using a third-party task manager replacement for Task List, you might (depending on its configuration) be able to hide all of its Windows-arranging and file functions within WinGuard.**

**6. V.2 does all of its work in the Windows environment, unlike V.1 (which switched to DOS briefly for some of its functions). (This change is also true for the V.2 installation and uninstallation programs, as well.)**

**7. V.2 should be able to function well with many networked computer configurations, unlike V.1 (which worked only within the directory structure of a typical non-networked machine).**

**8. V.2 does not display the password as it is entered (unlike V.1), so that an onlooker will not be able to read what the password is. In fact, if you type either a period or a comma immediately after entering your password, you may then type several more "decoy" characters; doing this would ensure that an onlooker would have trouble even counting how long the password is. (For example, if you were to enter the password as "shield,aeiou&#$123", WinGuard would read it as just "shield".)**

**9. V.2 uses a file to store the working password, as did V.1, but the name of the file (wngrd.dll) is now a "disguise". (Who ever tries to view a .dll file, anyway?) Furthermore, the password itself is coded in the V.2 file, so it's unlikely that anyone could figure out what the password actually is, in any event.**

**10. V.2 does not need to hide its files in a hidden directory, as did V.1. Without sacrificing any security advantage, V.2 is able to function effectively yet unobtrusively in either the Windows directory or the Windows System directory.**

**11. V.2 is written in Visual Basic 3.0, and is a better overall program than was V.1. However, V.2 does require the presence of vbrun300.dll in the Windows System directory, and it does use more memory than V.1. Because of this, a PC with only 1 MB of total memory (with no extended memory) is not likely to be able to run WinGuard V.2, even though it may have (barely) run V.1. (Note, of course, that WinGuard uses memory only when you actually run it, and that its protections require essentially no memory themselves.)**

**As you can see, if you have used Version 1 of WinGuard, there have been quite a few improvements made in Version 2. Upgrading from Version 1 will provide previous users with more flexibility and more security than they had before. However, despite all these changes, if you have been using V.1, do not panic; you will find that the same protection level scheme is utilized in V.2. Thus, if you have experimented a bit, and finally settled on one particular protection level setting for your computer(s), you will find that V.2's setting will have the exact same effect. The only change that you will notice is that WinGuard V.2 lets you do so much more than V.1, so that you probably will end up doing a little more experimenting.**

## INSTALLING WINGUARD

**The easiest (and recommended) way to install WinGuard is to run the installation utility,**

**install.exe, located on the WinGuard program disk or in the directory in which winguard.zip was "unzipped".  For those that wish to know what occurs during installation, or for some reason are not able to use install.exe (and wish to install WinGuard manually), a list of events that occur during normal installation now follows:**

**1.  Install.exe checks for the version of Windows that is installed;  since WinGuard will not work properly with Windows versions earlier than V.3.1, install.exe will terminate (with a message) if the installed Windows version is older.**

**2.  Install.exe tries to detect three paths:  the location of the source files, the location of the Windows directory, and the location of the Windows System directory.  The user is asked to confirm (or correct) the detected paths.  Note that, on most non-networked computers, the Windows directory will typically be c:\windows, while the Windows System directory will typically be c:\windows\system.  However, a networked computer will likely have a very different arrangement, with the Windows directory being something like, say, q:\yourname, while the System directory might be something like g:\windows.**

**3.  Install.exe checks the three paths for the presence of vbrun300.dll, a file needed by Visual Basic programs.  It must be found in the Windows or Windows System directory for WinGuard to run, so if it is not already there, and is not found with the source files (and vbrun300.dll is not routinely distributed as part of winguard.zip over bulletin board systems), then install.exe ends with a message pointing out that a copy of vbrun300.dll must be placed there.  Note that vbrun300.dll IS found on the WinGuard program diskette, and will (if necessary) be copied to either the Windows directory (on a networked computer) or to the Windows System directory (on a non-networked PC) later on in the installation.**

**4.  Install.exe looks for an earlier version of WinGuard on the hard disk.  If one is found, it is removed before the newer version of WinGuard may be installed.**

**5.  Install.exe makes backup copies of three Windows .ini files (copying progman.ini to progman.wgd, control.ini to control.wgd, and win.ini to win.wgd).**

**6.  Install.exe copies the following files to either the Windows directory (on a networked computer) or to the Windows System directory (on a non-networked PC):  winguard.exe, winguard.hlp, winguard.dll, winguard.txt, wngrdpwd.txt, educator.txt, whatsnew.txt, regform.txt, and vbrun300.txt.  Wngrd.dll and vbrun300.dll will also be copied there, if not already present.  Cmdialog.vbx will be copied there, as well, unless a newer version of this file is already present.  Install.exe will terminate with a message if any file is not copied properly.**

**7.  Install.exe gives the user the chance to create a WinGuard group in the Program Manager window (strongly recommended, unless one is already present, as this is the easiest way to become familiar with WinGuard's features).  If the "go ahead" is given, install.exe will have makgroup.exe (also found among the source files) create the new group, concluding the installation.**

**If the installation program was not able to automatically create a WinGuard Program Manager group for you, or if you elected at the time of installation not to create one (but wish to do so now), here are steps you may follow:**

**First, you might try running makgroup.exe (on the WinGuard program diskette, or in the winguard.zip directory);  this is the program that install.exe would call to create the program group, and it may create the group for you now.**

**Or, you might try copying the file winguard.grp (on the WinGuard program diskette, or in**

**the winguard.zip directory) to the Windows directory. Then, select the File Menu in Program Manager, then New, and then Program Group. When you obtain a Program Group Properties dialog box, enter WinGuard for the Description, and winguard.grp for the Group File. Click on OK, and you should see a complete WinGuard group appear.**

**Note that certain installation files, such as install.exe and makgroup.exe, are not copied to the hard disk, nor is the uninstallation program, uninstal.exe. Winguard.wri, an expanded version of winguard.txt, is also not copied to the hard disk, for security reasons, as it contains details of WinGuard's functions of which a guest user should not be aware.**

**WinGuard may be run from winguard.exe, which should be in the Windows directory (on a networked computer) or in the Windows System directory (on a non-networked computer). Once WinGuard is up and running, you may explore the following various features:**

## PROTECTION LEVELS

**WinGuard may be utilized by the authorized user to configure Program Manager for any one of seven increasingly restrictive protection levels, or to return it to its default zero-protection setting. These safeguards run from merely preventing spatial changes from being made by the guest user to bringing about the total inactivation of virtually all Program Manager file functions.**

**Each protection level change is accomplished by first activating the appropriate WinGuard protection level command button (or menu item), and then restarting Windows (which may also be done from within WinGuard).**

### PROTECTION LEVEL 0

**Protection Level 0 provides no protection against changes made to Program Manager. (This, of course, is Program Manager's normal, default state, which WinGuard was designed to modify.) Although one of the other protection levels would be more suitable for most security purposes, Level 0 must still temporarily be invoked for those Program Manager changes that the authorized user must occasionally make.**

**Protection Level 0 may be applied by using either the Level 0 command button or the Unprotect button (or by using either of the corresponding menu items). Windows must be restarted before the level change will take effect.**

### PROTECTION LEVEL 1

**Protection Level 1 will "dim" the Save Settings on Exit command in the Program Manager Options Menu, preventing the desktop from being permanently rearranged. Under this protection level, spatial modifications to Program Manager may still be temporarily made, but it becomes impossible to save those changes. Therefore, the next time that Windows is started, Program Manager will come up with the original desktop layout intact.**

**It should be noted, though, that Level 1 does not protect against either the creation or deletion of groups, nor does it protect against the creation, deletion, or moving of individual items, or against changes to their properties.**

**Protection Level 1 may be applied by using the Level 1 command button (or by using the corresponding menu item). Windows must be restarted before the level change will take effect.**

### PROTECTION LEVEL 2

Protection Level 2 will prevent the deletion of existing Program Manager groups, or the creation of new groups, as well as maintaining the protections offered by Level 1. When an attempt is made to use the File Menu's New, Move, Copy, or Delete commands while the focus is on a group, it will be found that they are "dimmed", as will be the entire Properties box.

Note, however, that no protection is provided against any changes to individual program items or to their properties under Level 2.

Protection Level 2 may be applied by using the Level 2 command button (or by using the corresponding menu item). Windows must be restarted before the level change will take effect.

## PROTECTION LEVEL 3

Protection Level 3 incorporates the safeguards of Levels 1 and 2, plus it will also prevent the deletion or creation of Program Manager items. If an attempt is made to use the File Menu's New, Move, Copy, or Delete commands, it will be found that they are "dimmed".

It should be noted, however, that Level 3 does not prevent the changing of any item's properties.

Protection Level 3 may be applied by using the Level 3 command button (or by using the corresponding menu item). Windows must be restarted before the level change will take effect.

## PROTECTION LEVEL 4

Protection Level 4 prevents modifications to the command line (which will be "dimmed") for any program item in the File Menu's Properties dialog box. Level 4 carries over all of the protection features of Levels 1, 2, and 3, as well.

Protection Level 4 may be applied by using the Level 4 command button (or by using the corresponding menu item). Windows must be restarted before the level change will take effect.

## PROTECTION LEVEL 5

Protection Level 5, besides maintaining the safeguards of Levels 1 through 4, will protect against the changing of any program item's properties, by "dimming" the New, Move, Copy, and Delete commands in the File Menu, as well as all of the entry fields in its Properties dialog box.

Protection Level 5 may be applied by using the Level 5 command button (or by using the corresponding menu item). Windows must be restarted before the level change will take effect.

## PROTECTION LEVEL 6

Protection Level 6 will "dim" the Run line in the File Menu, thus preventing one from starting a program not already present as an icon in Program Manager. Since Level 6 carries over all of the protections provided up through Level 5, the only functional commands in the File Menu will be Open, Properties, and Exit Windows (and the Properties option will only be informational in function, since the entire Properties dialog box will be "dimmed").

Protection Level 6 may be applied by using the Level 6 command button (or by using the corresponding menu item).  Windows must be restarted before the level change will take effect.

PROTECTION LEVEL 7

Protection Level 7 removes the entire File Menu from Program Manager, as well as preserving all the safeguards provided by Levels 1 through 6, providing the maximum level of protection against Program Manager changes.

Protection Level 7 may be applied by using the Level 7 command button (or by using the corresponding menu item).  Windows must be restarted before the level change will take effect.

## NO WINDOWS CLOSE

WinGuard's Options Menu includes a No Windows Close command item, as well as an opposite Allow Windows Close item.

Checking the No Windows Close menu item will prevent the guest user from exiting Windows by any usual means;  once the command is in effect, the File Menu's Exit Windows command and the Control Menu's Close command will both be "dimmed", and double-clicking on the Control Menu Icon will also become ineffective for closing Windows.

Checking the Allow Windows Close menu item will enable exiting from Windows by the normal means, either by using the File Menu's Exit Windows command or the Control Menu's Close command, or by double-clicking on the Control Menu Icon.

Even if the No Windows Close command is in effect, the authorized user still has the ability to exit from Windows from within WinGuard, by using either the Exit Windows command button or the Exit Windows File Menu item.

Note the Windows must be restarted before either the No Windows Close command or the Allow Windows Close command will take effect.

## PROGRAM MANAGER GROUPS

WinGuard provides the opportunity for the authorized user to hide one or more of the program groups (such as Main, Accessories, Applications, etc.) shown in the Program Manager window, preventing the guest user from accessing (or perhaps even knowing about) any such groups, once protected.  If the authorized user needs to redisplay any hidden group, this may be done easily from within WinGuard, although this does require restarting Windows (but this may also easily be done from within WinGuard).

If it is desired merely to hide a few selected icons that are present in several different groups, it might be advantageous to create a Program Manager group just for them, and then to move each of them to the new group (by dragging and dropping with the mouse), before hiding the group with WinGuard.  If you elected to have a WinGuard group created for you during installation, you may use that group for the one to hide (after copying or moving WinGuard's own icon to another group, of course, in order to access WinGuard after the WinGuard group has been hidden).

By the way, if you are not yet familiar with drag-and-drop procedures, you might wish to know that you may copy or move Program Manager icons from one program group to another by using just the mouse.  For example, if you point at an icon, and then click on it with the left mouse button, you may drag it (by continuing to hold the button down) to another group, and then drop it there (by releasing the button), in order to move it.  If you hold down the Ctrl key while performing the above procedure, you will copy the icon, instead of moving it.

Note that Windows must be restarted before any program group display change (either hiding a visible group or redisplaying a hidden group) will take effect.

Of course, WinGuard's companion security program, ProGuard, allows password-protecting one or several individual icons, without having to remove them from sight, still allowing for quick access to them by the authorized user.  (See the section further below on ProGuard Introduction for more information on this related security program from Cetus Software.)

## CONTROL PANEL ICONS

WinGuard provides the opportunity for the authorized user to hide one or more of the icons in the Control Panel window, preventing the guest user from accessing the Program Manager settings for such features as colors, drivers, fonts, printers, virtual memory, and desktop details (such as wallpaper or screen savers).

In order that the authorized user may still obtain access to any Control Panel icons that are hidden, WinGuard's Control Panel Icons Window provides command buttons for all of the regular Control Panel functions, whether hidden or otherwise.

Note that any changes made in Control Panel icon display will already be in effect the very next time Control Panel is opened (unlike WinGuard's other protections, which require restarting Windows before taking effect).

## REPLACING TASK LIST

Ordinarily, Windows Task List (Task Manager) may be started by double-clicking on the Windows desktop, as well as by activating the Switch To command in the Control Menu of many Windows applications.  However, the authorized user has the option of replacing such access to Task List with easy access to WinGuard, instead.  That is, double-clicking on the desktop would bring up WinGuard rather than Task List.  (WinGuard would still require the proper password, of course.)

Besides increasing the ease of accessing WinGuard, this change would be most useful on a computer with a third-party task manager (with window and file functions) installed, which the authorized user might wish to shield from the guest user.

Task List may be replaced by clicking on the Replace Task List command in WinGuard's Main Window Options Menu, and the change may be negated by clicking on it once again.  If WinGuard has been so set to replace Task List, a checkmark will appear next to the menu item, which will disappear when normal access to Task List has been restored.  Note that Windows must be restarted for the actual change to take effect.

Even after making this change, the authorized user would still be able to invoke Task List (or a task manager) from within WinGuard, by activating the Switch To command button in WinGuard's Main Window (or the corresponding menu item).  (Technically, Task List is not actually replaced, as it is only the access to it that has been changed, having been switched to WinGuard instead.)

It is a simple matter at any time for the authorized user to have WinGuard restore normal access to Task List, and even to certain custom task manager installations.  However, if WinGuard detected that a third-party task manager was installed on the computer in such a way that WinGuard would not have been able to restore it, then the Replace Task List menu command would have been disabled.

## WINGUARD SECURITY

In order to restrict access to WinGuard and the programs that it protects, it is necessary for the authorized user to use a password.  For the shareware version of WinGuard, the default password at the time of initial installation is "shield", but this should be changed to one of the authorized user's own choosing as soon as possible.  The actual working password is stored in a file, wngrd.dll (in the Windows System directory), in coded form.

If the authorized user ever forgets the working password, or if the password file becomes corrupted, wngrd.dll may be deleted;  WinGuard may then be started by using the default password of "shield", and the working password may then be chosen once again.  (Note that the registered version of WinGuard comes with a private default password chosen by the registered user at the time of registration.)

The password may be changed at any time from within WinGuard after the correct working password has been entered.  The password must consist entirely of letters (not case-sensitive) and/or numbers, with no spaces or punctuation, and is limited to twenty characters.

To make it more difficult for someone else to see the password as the authorized user enters it, the password itself does not appear on the screen (except when the working password is actually being changed, which should be done in private).  Furthermore, if either a period or comma is typed at the end of the actual password, several "decoy" characters may be entered immediately afterward (as WinGuard will only read the characters up to the period or comma), so that someone watching the password being entered would have trouble even counting how long the password actually is.

## OBTAINING HELP

WinGuard provides several ways to obtain help, including (but not limited to) this file.

If you click with the right mouse button on any Main Window command button, you will find that you may obtain context-sensitive help from WinGuard's main help file, without having to go to the help contents first to find the topic.  You may also receive help for a specific WinGuard control by pressing the F1 key while that feature has the focus, or you may simply use the Help Menu in any of the WinGuard windows.

You may move from one topic to another in WinGuard's main help file by clicking with the mouse on any item that is underlined.  From the keyboard, you may use the Tab key to highlight an underlined item, and then press Enter.  While viewing WinGuard's help file, you may learn more about how to use a Windows help file in general by pressing the F1 key, or you may choose "How to Use Help" from the help file's own Help Menu.

You will find, as you use WinGuard's Main Window, Program Manager Groups Window, or Control Panel Icons Window, that the text message in the Status Bar at the bottom of the window changes as you move the mouse (or change the focus with the Tab key).  In the Main Window, the Status Bar will show the current protection level at start-up (regardless of where the cursor is or where the focus is), and at any time the mouse is moved over the

**Main Window's background. Otherwise in the Main Window, or throughout the Program Manager Groups Window and the Control Panel Icons Window, the Status Bar will provide a short message relating to the command button that the mouse cursor is over (or to which the Tab key moves the focus).**

**By the way, WinGuard actually comes with two help files. One is named winguard.hlp, but that is not actually the name of the main help file. For security purposes, winguard.hlp is just a small help file with only one window that warns the guest user about WinGuard's password protection, and is the only file that is accessed by using the F1 key before the correct password has been entered. However, once the correct password has been typed in by the authorized user, the main help file (which is actually named winguard.dll) comes up, instead, whenever Windows help is invoked by any one of the above methods.**

## EXITING WINGUARD

**WinGuard provides several way to close itself, depending upon the circumstance. It is possible to close WinGuard and then return to Windows, either with or without saving any protection level changes that may have just been made. It is also possible to close WinGuard and then to either exit or restart Windows, to bring about desired Program Manager protection level and/or group changes immediately.**

**The Protect Now command will restart Windows with the currently selected protection level in place. The Unprotect Now command will restart Windows with Level 0 in place, regardless of the current protection level setting.**

**The Cancel Changes command will close WinGuard and then return to Windows, after first undoing any protection level changes made during that running of WinGuard. Note, however, that the Cancel Changes button will undo only protection level changes, not program group changes or Control Panel icon changes (which must be undone individually, using the Program Manager Groups Window or the Control Panel Icons Window).**

**The Exit Windows command will close WinGuard and then exit Windows, activating the currently selected protection level. The Exit WinGuard command will close WinGuard and then return to Windows, to have any changes made in Program Manager groups or protection level take effect the next time that Windows is started.**

## WINGUARD'S WINDOWS

**WinGuard involves five windows, as follows:**

**The center of the WinGuard program is the Main WinGuard Window. One of the other windows is an opening windows that leads to the Main Window, and the other three windows are accessed from within the Main Window.**

**The opening window is the Password Entry Window. which must be gotten past by the proper entry of a password before reaching the Main Window.**

**The principal functions of WinGuard's Main Window include setting the Program Manager protection level, accessing "sensitive" Windows programs that may be hidden within WinGuard, reaching other WinGuard windows, and exiting from WinGuard.**

**Accessible from the Main Window are windows for controlling the visibility of Program Manager program groups, controlling the visibility of Control Panel icons, and changing the WinGuard working password.**

You should explore the features and functions of each window, referring to the on-line help file for assistance.  Some experimentation will be necessary before you will be able to have your computer configured with exactly the protections it needs for your particular situation.

## WINGUARD'S CONTROLS

The following is a list of command buttons, menu items, and other WinGuard control features, for reference when using WinGuard:

### ALLOW WINDOWS CLOSE

The Allow Windows Close menu item may be used to enable exiting from Windows by the normal means, either by using the File Menu's Exit Windows command or the Control Menu's Close command, or by double-clicking on the Control Menu Icon, undoing the protection offered by the corresponding No Windows Close menu item.  Note that Windows must be restarted before the Allow Windows Close command will take effect.

### BUTTON BAR

The button bar is the row of command buttons at the top of the Main WinGuard Window. Each button invokes one of the various Windows functions and utilities that the authorized user might wish to remove from Program Manager, but would still have access to within WinGuard.

### CANCEL BUTTON

In the Password Entry Window, the Cancel command button may be used to exit WinGuard before accessing the Main WinGuard Window.

In the Password Change Window, the Cancel command button may be used to return to the Main Window without accepting a new password.

### CANCEL CHANGES BUTTON

The Cancel Changes command button in the Main WinGuard Window (or the corresponding Options menu item) will close WinGuard and then return to Windows, after first undoing any protection level changes made during that running of WinGuard.  Note, however, that the Cancel Changes button will undo only protection level changes, not program group changes or Control Panel icon changes.

### CLOSE BUTTON

The Close button, found in both the Program Manager Groups Window and the Control Panel Icons Window, is used to return to the Main WinGuard  Window.  The Close button has no effect on any changes that may have been made within its parent window.

### CONTROL PANEL BUTTON

The Control Panel command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access Windows Control Panel, allowing the authorized user to remove its icon from Program Manager (for security purposes, if so desired), but still enabling him/her to reach the utility through WinGuard.

**CONTROL PANEL ICON BUTTON**

**The Control Panel Icons command button in the Main WinGuard Window (or the corresponding Options menu item) may be used to access the Control Panel Icons window, in order to hide or show individual Control Panel icons in Control Panel's own window.**

**DESELECT BUTTON**

**In the Program Manager Groups Window, the Deselect command button may be used to deselect any Program Manager group that has been selected in either the Visible Groups listbox or the Hidden Groups listbox.**

**DOS PROMPT BUTTON**

**The DOS Prompt command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access DOS, allowing the authorized user to remove the DOS Prompt icon from Program Manager (for security purposes, if so desired), but still enabling him/her to easily reach it through WinGuard.**

**EXIT WINDOWS BUTTON**

**The Exit Windows command button in the Main WinGuard Window (or the corresponding File menu item) allows the authorized user to exit from Windows from within WinGuard. (This would be especially useful with Protection Level 7, which removes the entire File menu, including the Exit Windows command, from Program Manager.)**

**EXIT WINGUARD BUTTON**

**The Exit WinGuard command button in the Main WinGuard Window (or the corresponding File menu item) will close WinGuard and then return to Windows.  Any Program Manager groups display or protection level changes made will take effect the next time that Windows is started.**

**FILE MANAGER BUTTON**

**The File Manager command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access Windows File Manager, allowing the authorized user to remove its icon from Program Manager (for security purposes, if so desired), but still enabling him/her to reach it through WinGuard.**

**FILE MENU**

**Within the Password Entry Window, the File Menu provides the OK and Cancel commands, which (like the window's command buttons) may be used to accept the password entered or to exit before reaching the Main Window.**

**Within WinGuard's Main Window, the File Menu contains menu items that duplicate the functions of the command buttons in the Main Window's button bar, and the functions of the Exit WinGuard and Exit Windows buttons, primarily for keyboard access to these commands.**

**Within the Password Change Window, the File Menu provides the OK and Cancel commands, which (like the window's command buttons) may be used to accept the new password or to exit before returning to the Main Window.**

**HELP MENU**

**Each of WinGuard's windows has a Help menu, where help on topics related to that window may be obtained.**

**HIDDEN GROUPS LISTBOX**

**The Hidden Groups listbox in the Program Manager Groups Window displays the program groups that have been set to be visible in Program Manager.**

**Any group may be moved to the Hidden Groups listbox by using the Hide command button or by double-clicking directly on it in the Visible Groups listbox.**

**Note that Windows must be restarted before any changes made, either hiding groups or showing groups, actually take effect.**

**HIDE BUTTON**

**In the Program Manager Groups Window, the Hide command button may be used to move any Program Manager group that has been selected in the Visible Groups listbox into the Hidden Groups listbox. (It is also possible to double-click directly on any group in the Visible Groups listbox to move it to the Hidden Groups listbox.) The next time Windows is started, any Program Manager group so moved will be hidden from view.**

**HIDE ICON OPTION BUTTONS**

**Within the Control Panel Icons Window, the Hide Icon option buttons are used to select which Control Panel icons are to be hidden from view.**

**LEVEL [ 0 - 7 ] BUTTONS**

**Each of the Protection Level command buttons in the Main WinGuard Window (or the corresponding Options menu items) may be used to set one of the Program Manager protection levels. Note that the protection level change takes effect the next time Windows is started. (See the earlier winguard.wri topic on Protection Levels for a description of the effect of each protection level.)**

**NO WINDOWS CLOSE**

**The No Windows Close menu item may be used to prevent the guest user from exiting Windows by any of the usual methods; once the command is in effect, the File Menu's Exit Windows command and the Control Menu's Close command will both be "dimmed", and double-clicking on the Control Menu icon will also become ineffective for closing Windows. (Even if the No Windows Close command is in effect, the authorized user still has the ability to exit from Windows from within WinGuard, either by using the Exit Windows command button or the Exit Windows File Menu item.) Note the Windows must be restarted before the No Windows Close command will take effect.**

**OK BUTTON**

**In the Password Entry Window, once the correct password has been entered in the Password Entry Box, the OK command button may be used to reach the Main WinGuard Window.**

**In the Password Change Window, once the new password has been entered in the Password Entry Box, the OK command button may be used to accept the new password**

and return to the Main Window.

**OPEN BUTTON**

The Open command button in the Main WinGuard Window (or the corresponding File menu item) may be used by the authorized user to access an Open dialog box, in order to run a program from within WinGuard.

**OPEN CONTROL PANEL ICON BUTTONS**

Within the Control Panel Icons Window, the Open Control Panel Icon buttons are used to open any of the Control Panel icons, including those that are hidden from view in Control Panel's window by WinGuard.

**OPTIONS MENU**

Several of WinGuard's windows have Options menus, which generally duplicate the functions of the command buttons within each window.

**PASSWORD ENTRY BOX**

In the Password Entry Window, the Password Entry Box is employed to enter the password used to access WinGuard. After the password has been entered, the OK command button should be pressed. The password must be entered correctly within three tries or the Password Entry Window closes itself.

In the Password Change Window, the Password Entry Box is employed to enter the new password, after which the OK command button should be pressed to return to the Main Window.

**PIF EDITOR BUTTON**

The PIF Editor command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access PIF Editor, allowing the authorized user to remove its icon from Program Manager (for security purposes, if so desired), but still enabling him/her to reach it through WinGuard.

**PROGRAM MANAGER GROUPS BUTTON**

The Program Manager Groups command button in the Main WinGuard Window (or the corresponding Options menu item) may be used to access the Program Manager Groups window, in order to hide or show individual Program Manager groups.

**PROTECT NOW BUTTON**

The Protect Now command button in the Main Window (or the corresponding Options menu item) will close WinGuard and then restart Windows, to have any change in the Program Manager protection level or group display settings take effect immediately.

**PROTECTION LEVEL [ 0 - 7 ] BUTTONS**

Each of the Protection Level command buttons in the Main WinGuard Window (or the corresponding Options menu items) may be used to set one of the Program Manager protection levels. Note that the protection level change takes effect the next time Windows is started. (See the earlier winguard.wri topic on Protection Levels for a description of the effect of each protection level.)

**RUN BUTTON**

**The Run command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access the Windows Run dialog box, allowing the authorized user to easily reach it through WinGuard. (This would be especially useful with Protection Level 6, which "dims" the Run command in the Program Manager File menu, or with Level 7, which removes the entire File menu, including the Run command.)**

**SHOW BUTTON**

**In the Program Manager Groups Window, the Show command button may be used to move any Program Manager group that has been selected in the Hidden Groups listbox into the Visible Groups listbox. (It is also possible to double-click directly on any group in the Hidden Groups listbox to move it to the Visible Groups listbox.) The next time Windows is started, any Program Manager group so moved will be returned to view.**

**SHOW ICON OPTION BUTTONS**

**Within the Control Panel Icons Window, the Show Icon option buttons are used to select which Control Panel icons are to be visible.**

**STATUS BAR**

**At the bottom of the Main Window, the Program Manager Groups Window, and the Control Panel Icons Window is a Status Bar (or Status Label), which is one way in which WinGuard provides help for various features in these windows.**

**You will find, as you use WinGuard's Main Window, Program Manager Groups Window, or Control Panel Icons Window, that the text message in the Status Bar at the bottom of the window changes as you move the mouse (or change the focus with the Tab key). In the Main Window, the Status Bar will show the current protection level at start-up (regardless of where the cursor is or where the focus is), and at any time the mouse is moved over the Main Window's background. Otherwise in the Main Window, or throughout the Program Manager Groups Window and the Control Panel Icons Window, the Status Bar will provide a short message relating to the command button that the mouse cursor is over (or to which the Tab key moves the focus).**

**SWITCH TO BUTTON**

**The Switch To command button in the Main WinGuard Window (or the corresponding File Menu item) may be used to access Task List (Task Manager), allowing the authorized user to easily reach it through WinGuard.**

**Ordinarily, Task List may be started by double-clicking on the Windows desktop, as well as by activating the Switch To command in the Control Menu of many Windows applications. However, WinGuard gives the authorized user the option of replacing such access to Task List with easy access to itself, instead.**

**If this change were made, the authorized user would still be able to invoke Task List from within WinGuard, by activating the Switch To command button in WinGuard's Main Window (or the corresponding menu item).**

**SYSTEM EDITOR BUTTON**

**The System Editor command button in the Main WinGuard Window (or the corresponding**

File menu item) may be used to access System Editor, allowing the authorized user to remove its icon from Program Manager (for security purposes, if so desired), but still enabling him/her to reach it through WinGuard.

UNPROTECT NOW BUTTON

The Unprotect Now command button in the Main Window (or the corresponding Options menu item) will close WinGuard and then restart Windows, with Protection Level 0 in place.

VISIBLE GROUPS

The Visible Groups listbox in the Program Manager Groups Window displays the program groups that have been set to be hidden in Program Manager.

Any group may be moved to the Visible Groups listbox by using the Show command button or by double-clicking directly on it in the Hidden Groups listbox.

Note that Windows must be restarted before any changes made, either hiding groups or showing groups, actually take effect.

WINDOWS SETUP BUTTON

The Windows Setup command button in the Main WinGuard Window (or the corresponding File menu item) may be used to access the Windows Setup utility, allowing the authorized user to remove its icon from Program Manager (for security purposes, if so desired), but still enabling him/her to reach it through WinGuard.

## UNINSTALLING WINGUARD

WinGuard may be uninstalled by using the utility, uninstal.exe, which should be found either on the WinGuard program diskette or in the winguard.zip file (or, probably the same place that this file was found).

PLEASE NOTE:  At the time that WinGuard is uninstalled, the following conditions MUST be present:

- WinGuard itself must NOT be running.
- NO other program (besides Program Manager or File Manager) should be running.
- WinGuard Protection Level 0 MUST be in effect.
- ALL Program Manager groups MUST be visible.
- WinGuard MUST be set to Allow Windows Close.
- ALL Control Panel icons MUST be visible.
- WinGuard must NOT be set for replacing Task List.

Basically, ALL of the protections that WinGuard offers should be defeated, returning Program Manager back to its normal, default state BEFORE attempting to uninstall WinGuard.

It is very important that ALL of the above be VERIFIED before uninstalling WinGuard.

## ABOUT CETUS SOFTWARE

Cetus Software is the creator of several Windows utilities, including ProGuard, StoreWindows, PadLock, Reveille, and Seasons, as well as WinGuard.  Shareware

**versions of these products may be found on several bulletin board systems, or may be obtained on diskette directly from Cetus Software for a nominal charge ($5.00 each, postpaid).**

**Please direct all inquiries regarding Cetus Software's products to:**

**Cetus Software**
**Post Office Box 700**
**Carver, MA 02330 USA**

**Internet: Fwcetus@aol.com**

**Cetus Software thanks you for trying out WinGuard !!!**

## STORMWINDOWS INTRODUCTION

**In addition to WinGuard, Cetus Software offers a related security program, StormWindows, offering essentially the same functions as WinGuard, but depending on an entirely different means of security. Like WinGuard, StormWindows can protect a Windows 3.1 computer from having any of its Program Manager groups or icons rearranged or damaged. StormWindows can also hide "sensitive" programs (such as Windows Setup, Control Panel, or File Manager), as well as selected Program Manager groups and Control Panel icons.**

**StormWindows' protections would probably be the most useful to someone in charge of a number of computers at a business or at a school. For security purposes, StormWindows is designed to perform its functions directly from a diskette, kept in the possession of the authorized user, and thus StormWindows can conveniently provide ideal protection to any number of Windows computers on display in a store, without requiring installation onto any of their hard disks.**

**The shareware version of StormWindows is available on several bulletin board systems, or may be obtained on diskette in uncompressed form, directly from Cetus Software (P.O. Box 700, Carver MA 02330 USA), for a nominal charge ($5.00, postpaid).**

## PROGUARD INTRODUCTION

**In addition to WinGuard, Cetus Software offers a related security program, ProGuard. Unlike WinGuard, which is intended to protect Program Manager itself, ProGuard is designed to password-protect individual Program Manager icons. Thus, while WinGuard is more "global" in its protections, ProGuard is more application-specific.**

**ProGuard is designed to make it impossible for a guest user to run selected programs by double-clicking on their icons in Program Manager. Once a particular program's icon has been protected by ProGuard, the guest user will find that attempting to run the program will cause ProGuard to run instead, and that a password will be needed before the actual program can be made to start.**

**Logical programs to protect might include Windows Setup, Control Panel, PIF Editor, System Editor, and File Manager (and most users will have other programs that they would wish to protect, as well). When ProGuard is installed, the setup program provides icons for the above programs, already protected by ProGuard (and it's a simple matter to add ProGuard's protection to any other application's Program Manager icon, as well).**

**The shareware version of ProGuard is available as proguard.zip on several bulletin boards**

**systems, or may be obtained on diskette in uncompressed form directly from Cetus Software (PO Box 700, Carver MA 02330 USA) for a nominal charge ($5.00, postpaid).**

## PADLOCK INTRODUCTION

**PadLock may be used to "lock out" unauthorized users from accessing Windows or any Windows application. While PadLock is running, no keyboard or mouse command will have any effect outside of the PadLock window itself. Entry of the proper password (chosen by the authorized user) is required to access any of PadLock's controls or to end its protection.**

**PadLock may be configured to "lock up" Windows automatically at startup, or PadLock may simply be run whenever the authorized user desires to "freeze" Windows (such as when leaving the computer unattended), preventing any access by unauthorized users. PadLock even provides the authorized user with the means to edit system files, and to exit Windows, restart Windows, or reboot the computer from within itself.**

**The shareware version of PadLock is available on several bulletin board systems, or may be obtained on diskette in uncompressed form, directly from Cetus Software (P.O. Box 700, Carver MA 02330 USA), for a nominal charge ($5.00, postpaid).**

## REGISTERING WINGUARD

**Please note: WinGuard is NOT "freeware" !!!**

**The shareware version of WinGuard is being distributed on a trial basis for evaluation purposes, and is not "crippled" in any way, so that you may fairly judge WinGuard thoroughly. You may install the unregistered, shareware version of WinGuard on any one computer, and then try it out for 30 days. After this trial period you MUST either register your use of WinGuard, OR uninstall it, removing it from that computer. If you do indeed find WinGuard to be a useful addition to your computer's hard disk, then you MUST register your use of the program; in doing so you will be entitled to receive on disk a copy of the latest registered version of WinGuard, without any "reminder screens".**

**On the registration form you are given the opportunity to choose your own private default password (the password that may be used to access WinGuard if the password file, wngrd.dll, is deleted). Selecting a private default password will prevent even other knowledgeable WinGuard owners from being able to access your WinGuard program. Note that the password must consist of no more than twenty letters (not case-sensitive) and/or numbers, with no spaces or punctuation. Note also that, if you do not choose a private default password, then the default password on your registered copy of WinGuard will remain as "shield". (Of course, the "regular" current password, coded into the wngrd.dll file, may be changed from within WinGuard by you at any time.)**

**A single-user Individual License for WinGuard may be obtained for $14.95. A Site License for the use of WinGuard on any number of computers at one specific institutional location may be obtained for $74.95. An individual who has registered a previous version of WinGuard may upgrade to Version 2 for $9.95; an institution that has registered a previous version may upgrade for $49.95. Note that the above prices include shipping costs.**

**An Individual License entitles one individual registered user to install and use WinGuard on any computer(s) that he/she personally owns, but he/she must NOT allow his/her registered copy of WinGuard to be installed or used on any other computer(s). A copy of WinGuard registered to an individual user may be installed and used on his/her own**

personal computer(s) at an institution, but that personal copy of WinGuard must NOT be installed or used on any other computer at that institution, whether belonging to another individual or to that institution.

A Site License entitles the registered institution (school building, business office, organization headquarters, etc.) to install and use WinGuard on any number of computers belonging to that institution at that specific location. Any institution with multiple locations MUST obtain a separate site license for EACH location. Any copy of WinGuard registered to a particular institution location may NOT be distributed beyond the boundaries of that institutional site.

However, any person is permitted (and, in fact, ENCOURAGED) to distribute the UNregistered, shareware version of WinGuard to others, as long as ALL of its files are distributed together. For further information on WinGuard registration, or to obtain on disk a copy of the shareware version of WinGuard for free distribution and evaluation, please contact Cetus Software (PO Box 700, Carver, MA 02330 USA; Internet fwcetus@aol.com).

CETUS SOFTWARE THANKS YOU FOR TRYING OUT WINGUARD !!!

## WINGUARD V.2 REGISTRATION FORM

(Please note: This registration form is available separately as the file, regform.txt, and it may also be viewed and/or printed directly from the WinGuard help file, winguard.dll. Or, you may provide ALL of the following registration information in a separate letter or purchase order, if you prefer.)

PLEASE TYPE OR PRINT CLEARLY :

Date ____________________________

Name of User (for Individual License) __________________________________________
(or)
Name of Institution (for Site License) __________________________________________
(If multiple Site Licenses are being obtained, please list on the back of this form.)

Mailing Address ___________________________________________________

Mailing Address ___________________________________________________

Mailing Address ___________________________________________________

Daytime Telephone Number (with Area Code) _____________________________

Default Password Choice ___________________________________
(Maximum of 20 letters or numbers, with no spaces or punctuation)

Please circle size of diskette desired: 3-1/2" 5-1/4"

Please fill in the appropriate line with the amount you are enclosing:

One Individual License @ $14.95 = $____.95

_____ Site License(s) @ 74.95 = $_____.___

**One Individual License Upgrade @ $9.95 = $___.95**

**_____ Site License Upgrade(s) @ $49.95 = $_____.___**

**(Massachusetts residents:  Please include 5% state sales tax.)**

**(Please note that the above prices include shipping and handling costs.)**

**Please send this registration form, along with payment (or purchase order) to:**

**Cetus Software**
**Post Office Box 700**
**Carver, MA 02330 USA**

**Cetus Software thanks you for your WinGuard registration !!!**

# GLOSSARY

**The following is a glossary of terms that may be helpful when using WinGuard:**

### Authorized User
**the person using a computer with WinGuard installed who, by the use of a password,  is able to modify and/or bypass WinGuard's protections**

### Button Bar
**the row of command button at the top of the Main WinGuard Window that provides access to several "sensitive" Windows features and utilities**

### Control Panel
**a Windows utility that allows access to the settings of many of Program Manager's features (and whose icons may be hidden from the guest user by WinGuard)**

### Desktop
**the screen area outside of any active window, usually toward the margins of the screen**

### Dimmed
**the visual appearance of a menu item that has been inactivated (also sometimes referred to as "grayed out")**

### DOS Prompt
**the name of a Windows icon that allows the user to "shell out" to DOS from within Windows (and which may be hidden from a guest user by WinGuard)**

### File Manager
**the Windows application that allows access to every program and data file on a computer (and whose icon may be hidden from the guest user within WinGuard)**

### Guest User
**any person allowed to use a computer with WinGuard installed who may be restricted by WinGuard from accessing certain functions and/or programs**

### Hidden Groups
**Program Manager program groups that are not visible to the guest user, but that still exist,**

and may still be redisplayed by the authorized user from within WinGuard

## Open . . .

**a Program Manager menu item that allows opening a file or starting a program, which may be disabled by WinGuard (but whose functioning would still be available to the authorized user from within WinGuard)**

## PIF Editor

**the Windows utility used for the configuring of Program Information Files (used for running DOS programs within Windows), and whose icon may be hidden from the guest user within WinGuard**

## Program Manager

**the default Windows shell, the user-friendly interface to which WinGuard offers several levels and types of protections**

## ProGuard

**ProGuard is the companion program to WinGuard, designed to password-protect individual Program Manager icons. (Please see the earlier winguard.wri topic, ProGuard Introduction, for a full program description.)**

## Protection Level

**one of a series of seven sets of user restrictions, offering varying degrees of security to Program Manager**

## Reveille

**Reveille is a Windows application that will play musical tunes, either on demand while it is running, or at start-up using command line parameters sent it by a separate timer or scheduler (one is included with Reveille). NO sound card is needed. Reminder messages may be included in the Reveille command line and will be displayed in its window. Tune files (many of which are included with Reveille) may be created and/or edited from within Reveille, and groups of tunes may be saved as compilation files. Reveille is available as shareware from Cetus Software.**

## Run . . .

**a Program Manager menu item that opens a dialog box to enter a command line, which may be disabled by WinGuard (but would still be accessible to the authorized user from within WinGuard)**

## Save Settings on Exit

**a Program Manager menu item that allows any user to preserve changes (authorized or not) made to Program Manager, and which may be disabled by WinGuard**

## Seasons

**Seasons is a small Windows application that will calculate and display the number of years, seasons, months, moons, weeks, and days between the current date and a user-selected date. Seasons will also display the current date and time, as well as allowing the user to easily change the system date or time. Seasons may easily be configured to color-coordinate with the Windows desktop color scheme, and Seasons color combinations may be saved for future use. Seasons is available as "charityware" from Cetus Software.**

## Status Bar

**the label at the bottom of the Main WinGuard Window that provides help on WinGuard features**

### StoreWindows
**ProGuard is a program similar to WinGuard, designed to protect Program Manager, but depending on its functioning entirely from a diskette to maintain its security.  (Please see the earlier winguard.wri topic, StoreWindows Introduction, for a full program description.)**

### Switch To . . .
**the Program Manager menu item that invokes Windows Task List (Task Manager), and which may be disabled by WinGuard (but would still be available to the authorized user from within WinGuard)**

### System Editor
**a Windows utility that allows for the editing of important DOS and Windows configuration files (autoexec.bat, config.sys, win.ini, and system.ini), and whose icon may be hidden from the guest user within WinGuard**

### Task List
**the Windows utility, also known as Task Manager, that allows a user to switch between running applications, and to rearrange certain aspects of Program Manager (and whose icon may hidden from the guest user within WinGuard)**

### Visible Groups
**Program Manager program groups visible to the guest user, and whose icons are accessible to the guest user, unless hidden by WinGuard**

### Windows Setup
**a Windows utility that allows access to several fundamental aspects of Windows (video mode, keyboard, mouse, and network settings), and whose icon may be hidden from the guest user within WinGuard**

### WinGuard
**THE program that will protect Program Manager and the applications accessible through it from damage done by a guest user**