TruSecure Anti-Virus Policy Guide
Version 3.6.0

Specific and Detailed TruSecure^{â} Corporation Anti-Virus Policy Suggestions
Revised October 1, 2000

This policy guide is designed to deal with all current types of viruses known to TruSecure Corporation as of the revision date of this document.

The policies are specifically designed to deal with:

- Boot Sector & Partition Table Viruses
- Executable File Viruses
- Multipartite, Parasitic, Stealth, Polymorphic Viruses
- Conventional Macro Viruses
- Active Communication-enabled viruses, Trojans and worms (such as Happy99, Melissa, BubbleBoy, and LoveLetter) as well those that may utilize vectors such as ActiveX and JavaScript(Kak.Worm).
- Malicious code that has been compressed by a 32-bit compressing program
- Self-updating malicious code

TruSecure Corporation policy suggestions are characterized as either primary controls or synergistic controls. Primary controls are the most important and effective stand-alone preventative technique and constitute TruSecure Corporation's principal policy recommendations for organizations. Synergistic controls function in a way that is analogous to the military strategy of defense-in-depth, which provides for redundancy and failure of particular controls.

When operating alone, individual policies, controls or screens may have limited value, but synergistically can be quite effective. When used in conjunction with other synergistic controls, serial screens behave according to Baye's theorem. Their cumulative effect improves with the use of each control and their use enhances the effectiveness of other, primary, controls.

TruSecure recommends the use of all synergistic controls that a site can easily implement without infringing on other business productivity. This includes controls that are easily tolerated by particular groups or sub-groups in an organization, even though other groups may have less tolerance for these same controls. For any given site, it is common to be able to find synergistic controls that have very low infringement and maintenance costs. Furthermore, effective synergistic controls tend to require less frequent updates in order to maintain their effectiveness.

> *We expect that many synergistic controls (below) will not be applicable for a particular site or for a particular group at a particular site. TruSecure Corporation does not encourage changing business practices in order to achieve these controls. Rather we encourage the use of all controls that can be easily applied to a given organization and all that can be applied to given sub-groups in an organization.*

Virus protection controls can be applied at various levels in an organization. Before macro viruses, there was no practical utility in any controls applied anywhere other than PC desktops[1]. With the advent of macro viruses, the utility of the application of some controls at the server level became evident. With the communication-enabled viruses, controls at places other than the desktop (especially the perimeter) gain additional value.

[1] For more discussion on the derivation and logic behind these statements, please see other support documents such as ICSA Labs anti-virus surveys, virus study, and virus cost models, available at www.trusecure.com.

ICSA Recommended Virus Controls

Desktop Systems

TruSecure Corporation Recommended Primary Controls at Desktop Anti-Virus Level:

1) ICSA Certified anti-virus software installed and running on at least 90% of desktop PCs[2].
2) Subscribe to an alert service, such as the *TruSecure Monitor*^{TM}
3) If alert service is available, update desktop anti-virus software (virus signatures) at least monthly and be prepared to perform emergency updates within two business days after an alert.

   NOTE: Updating virus signatures is not good enough if you are using outdated software, please be certain you are using the most up-to-date version of your anti-virus software also.
4) If alert service is not available, update desktop anti-virus software weekly, or as often as your anti-virus vendor provides updates[3].
5) Educate users on how to update virus signatures where the process is not centralized.
6) Recommended desktop anti-virus software configuration:
   a. Full-time, background, real time, auto-protect or similar mode—ENABLED
   b. Start-up scanning of memory, master / boot records, system files—ENABLED
   c. Configure your AV to scan "All Files".
   d. Logs should be ENABLED to log all desktop virus-related activity.
7) Recommended desktop security settings that relate to viruses
   a) Ensure that all relevant Microsoft security patches and Service Releases are installed. See Annex xx for a list of such Security Patches and Service Releases.
   b) Turn off the Operating System Windows Scripting Host

      Go to Control Panel

      Select Add/Remove

      Under the Accessories Details, you will find a Windows Scripting Host checkbox.

      Clear the check box and the Windows Scripting Host will be removed from your computer.
   c) See E-mail client primary controls (below)

Additional notes on desktop level policies:

1) Alerts to users are neither recommended nor discouraged. TruSecure Corporation marginally recommends turning user alerts off, but system administrator alerts, logs, or other advisories on.
2) Daily, startup, login, or other periodic scanning of hard drives has little incremental utility. TruSecure Corporation recommends these options be turned off as their user infringement normally outweighs their protective value.
3) User-driven scanning policies such as requesting users to scan floppies, downloads or hard drives are not recommended as they are generally more expensive and infringing than useful.
4) Write protection of floppies is probably still worthwhile. There is little on the downside of a

[2] ICSA Labs virus surveys and cost models show a cost minimum when 90% of desktops have active protection with communications-enabled viruses. The same survey indicates that at upwards of 10% of machines with anti-virus products installed have the AV software turned off or other wise inoperable, therefore it is important to monitor AV protection to maintain this 90% coverage. This is up from 75% in v3.01 and earlier policy guides.

[3] Previous policy recommendations suggested quarterly updates when using alert capability or monthly updates without alert capability for macro level viruses and six month updates with alert capability, quarterly without, for pre-macro viruses.

policy of write-protection, and although the incidence of boot sector viruses seems to be declining, it is quite likely that future Win32 viruses will seek out the boot sectors of floppies. It will be easier to simply keep doing the write protection than to try suddenly to retrain everyone.

5) Educating users to look for virus-like activity is not a viable policy.

TruSecure Corporation Recommended Synergistic Controls at the Desktop-Level:

Implement as many of these as may be feasible within your organization.

(For items 1 & 2 specific recommended configuration settings are listed in Annex 1

1) Configure all instances of MS Word to save files as: Rich Text Format (*.rtf).

   Note 1: Renaming the *.doc file to *.rtf is not useful. Files must be saved in *.rtf format but may be saved by any file name or extension.

   Note 2: The policy should allow users to save as *.doc type where needed to reduce the file size of complex documents, or for files that require macro use or other very advanced, embedded features use. Otherwise, all files should be saved, mailed, stored, and maintained as *.rtf files by default.

2) ENABLE Macro Virus Protection in Microsoft Office Programs.

3) Seriously consider the use of add-in tool, which is designed to prevent double-click execution of e-mail attachments without challenge. Further, consider the permanent blocking and/or quarantining of executable files as attachments. If there is a real need to send or receive an executable program, arrangements can be made send the file compressed or encrypted with safeguards to prevent automatic or accidental execution and possible infection or damage. This can also offer some protection against malicious code hidden by 32-bit self-compression, such as Explore.Worm.MiniZip.

   For and example of an add in tool, see:
   Mail Add-on to Outlook 97 home page with link to file.
   http://www.microsoft.com/security/bulletins/mailaddon.asp
   Actual link to file...
   http://www.microsoft.com/security/downloads/attchwrn.exe
   NOTE: May not effective for Outlook 98 or Outlook 2000 client –This software has not been tested for effectiveness by ICSA Labs.

4) Configure WordView or WordPad as default association with *.doc files. Note: This is probably not effective on all versions and service releases of Office, particularly as the document-centric model becomes more common, but there is little on the downside. (Document-centric means that, instead of the user having to decide what program they want to use to examine a file, the operating system examines the file internally, as opposed to just looking at the extension, and decides what program should be used automatically. This already happens for some versions of some applications)

5) *Never* double-click on email-attachments. If you receive a document or spreadsheet that you want to look at, manually open it with WordView, Wordpad or XLView. If the attachment appears to be an executable program, *never* run it, despite what the accompanying email says, and no matter from whom it is received. It is now a common ploy for spreading viruses to make it appear it is from someone you know and trust. A viable policy is to ask users to never double click on an attachment unless they are *expecting it*.

6) Use AV software heuristic controls (in full-time background mode where available)

7) Set site attributes to READ ONLY for *.exe and *.dll in the %systemroot% directory. On Windows '9x machines, the usual directory is C:\Windows; on Windows NT and Windows 2000 machines, this is usually C:\WINNT. On Windows '9x machines this is done using the DOS command ATTRIB.EXE, on Windows NT and Windows 2000 machines, this is a permission

setting. Set site attributes for WSOCK32.DLL to “read only.”

8) Set AV product to alert or prevent changing of DOS Read-Only file attributes.
9) Store NORMAL.DOT (the default document template) in a protected folder on the file server or write-protect on the C: drive (i.e. set its “read only” attribute).
10) Create a copy of NORMAL.DOT, rename it and store it somewhere else on your computer, and create a batch file which runs from the AUTOEXEC.BAT, and which compares the two files. You can use a simple DOS command like FC (File Compare). NORMAL.DOT shouldn’t change, unless you are making some sort of customizations. While viruses may still defeat the read-only attribute on NORMAL.DOT, it is unlikely they will find the renamed copy. This would provide a useful early warning that something had happened.
11) Make a copy of Winsock.DLL and Kernel32.DLL and store them somewhere, and compare them the same way as the previous item, for the same reason. This would help protect against the likes of Happy99, which modifies Wsock32. Kernel32.dll is another likely target for malicious code. Periodically, we will probably suggest other candidate system files, which are both static, and thus defendable, and important, and thus likely targets. Windows 2000 implements a feature called Windows File Protection. This feature ensures that any protected file which is replaced, for any reason by any means, is automatically recovered from a protected cache.
12) Consider use of alternative word processor or office suite or limiting the use to certain users, providing other users with alternate applications. Remember that no product is bulletproof, and anything that becomes very popular is likely to be targeted.

E-Mail Client (Desktop) Applications

TruSecure Corporation Recommended Primary Controls at the E-Mail Client Level:

1) **Outlook:**
   a) Set Internet Explorer (IE) 4.x/5.x security settings in the Internet zone to "high"
   b) Customize IE settings (after setting to High) and disable ActiveX and Active Scripting -- set to disable (strongest) or prompt.

   Note 1: All versions of Outlook (except Outlook 97) rely on the Security Zone Security Settings from Internet Explorer (Tools, Internet Options, Security). Outlook lets you specify one of two zones to use as the security settings for dealing with email messages (Tools, Options, Security). You can use the Internet Zone (default), or the Restricted Sites Zone (which is more secure). You should be using the Restricted Sites Zone. But, as configured by default, Restricted is not strict enough. To the Restricted Sites Zone You should add these restrictions:
   1. Change Script ActiveX controls marked safe for scripting to disable / prompt
   2. Change Active Scripting to disable or prompt
   3. JavaScript settings should already be set to disable or prompt

   Note 2: RAMIFICATIONS -- of disabling Active Scripting probably include the inability of the machine to utilize Microsoft automated path update systems. Ramifications of disabling ActiveX and JavaScript mostly relate to web browsing infringements. If a company want its users to have tha ability to use Microsoft’s Windows Update feature, this may be overcome this may be overcome by including those pages in Internet Explorer’s Trusted Sites Zone.

   c) For Outlook ’98 users, disable the Preview Pane on all folder views. Since Preview Pane is enabled by default, this must be done for every folder available to the user. It must also be done again each time a new folder is added. By default, Outlook 2000 prevents the use of Active Scripting in the Preview Pane, regardless of the Security Zone setting of the Outlook 2000 client. However, it may be recommended that all users use the AutoPreview feature rather than the Preview Pane for consistency within the company.
2) **Outlook Express –** Disable Open and /or Preview panes. (Auto Preview which shows the first 3

lines of the message is probably ok and is certainly the safest of the three choices)

a) Perform IE Security Zone settings as above.

b) To disable the Preview Pane in Outlook Express:

1. Select Local Folders, then on the Menu Bar select View | Layout |
2. At the bottom of the Dialogue Do not check Preview Pane

3) **Netscape -** Disable JavaScript

To disable JavaScript: On the Menu Bar select: Edit | Preferences

a) On the left menu of the Dialogue Box Click Advanced

b) On the right side of the Dialogue Box, **Do Not Enable** JavaScript for e-mail and news.

c) For maximum safety, also disable JavaScript for browsing.

Note: Be advised, however, that Netscape uses JavaScript as part of its Smart Update program and will need to be Enabled to take make use of this feature.

4) **Other Email client** -- Disable Visual Basic Scripting or Java Scripting if utilized. Also, disable the use of IE for HTML viewing of e-mail if used by the client. (i.e. Eudora 4.x). If IE is on desktop, set as above.

Synergistic Controls at the E-Mail Client Level:

Implement as many as are feasible within your organization.

1) Turn off auto-open attachments
2) Configure for Plain text only
3) Configure to challenge execution of all executables attachments, see Annex Three
4) Configure to challenge opening of all *.doc, *.xls (and potentially *.ppt files)
5) Configure to challenge double click of all attachments
6) Consider using non MS Mail application
7) Do not store ALL_Company alias in local email lists

Network File and Print Servers

TruSecure Corporation Recommended Primary Control at Inside Server level:

1) Run AV Scanner in full time, background, automatic, auto-protect or similar mode on any file server which potentially stores files which are potentially infect-able such as*.doc files and executables which run on desktops.

Note: Daily or other periodic scanning has little value when auto-protect mode or similar full time mode is enabled.

2) Update server signature files monthly if alert service is available, weekly (or at maximum vendor rate) if no alert service is available.

Synergistic Controls at the Inside Server Level:

Implement as many as are feasible within your organization.

1) Utilize centralized AV management
2) Use centralized desktop management
3) Manage Internet Explorer and Visual Basic Scripting Centrally

E-Mail Gateways, Firewalls, Other Gateways and Anti-Spam Tools

TruSecure Corporation Recommended Primary Control at the Gateway Level:

1) Install e-mail gateway anti-virus software configured for full-time active mode.

2) Configure your anti-virus “Files List” to include scanning all files (most effective).
3) If you determine not to configure for scanning all files, check ANNEX Three for a list of files that may be automatically invoked.
4) Filter all arriving (and departing if possible) e-mail traffic by subject line /header:
5) Be prepared to rapidly adjust filtering rules (within 1 hour of notice for emergency alerts.
    a) Kill all mail with the following subject lines:
        - Important Message From* (for Melissa)
        - BubbleBoy is back!” (for BubbleBoy)
    b) Kill all mail with the following message header:
        - X-Spanska: Yes (for Happy99)
    c) Kill all mail with Message body text:
        - This document is very Important and you've GOT to read this !!! (W97M/Prilissa)
        - Here's some pictures for you! (W32/MyPics)
6) For additional help with sendmail see: http://www.sendmail.com/blockmelissa.html
7) For help with John Hardin's Procmail see: ftp://ftp.rubyriver.com/pub/jhardin/antispam/procmail-security.html
8) For help with Innosoft's PMDFsee: http://www.innosoft.com/iii/pmdf/virus-word-emergency.html

Gateway Level, Potential Synergistic Controls

Implement as many as are feasible within your organization.

1) Consider filtering all arriving and departing e-mail by spam threshold (greater than 40 identical messages blocked and source traced, if inside).
2) Filter all *.exe attachments and similar
3) Filter all *.doc and similar attachments
4) Filter ActiveX and JavaScript

Human Factors

TruSecure Corporation Recommended Primary Control at the Human Factor Level: None

Human Factors Potential Synergistic Controls:

Implement as many as are feasible within your organization.

1) Educate users to consider e-mail attachments and links potentially dangerous and to treat them very cautiously. Specifically recommend education: Open only expected attachments and links from known and trusted sources. Delete or question all others before opening
2) Keep system managers updated and informed. Links to hundreds of sites and related documents are available at http://www.icsa.net/virus.
3) Reinforce the message to users to never double click an e-mail attachment that is not expected. This policy is difficult since the affected (malicious) email will normally come "From" a trusted person. (Well informed users can be taught that *.doc, *.exe, *.doc, *.vbs, and *.hta extensions are the most likely to be dangerous). Desktop anti-virus software will normally work if it is kept updated and properly configured to operate full-time in the background.
4) E-mail containing Christmas card attachments, video, audio or other "fun attachments" and sexually-oriented attachments are likely to be the most exploited vector for this and similar viruses in the next two months.

Other Notes:

Diversity of your site compared with average sites with popular software in general is protective. Look for things about your site that change enough of your implementation of word processing, document file usage, e-mail, and other similar systems so as to not be identical to the average site.

ActiveX and JavaScript viruses have not yet materialized as real risks that have been experienced by the computing community. TruSecure Corporation believes that these vectors are imminent. Building defenses for them now will save the day when they become real. Viruses and worms dependent upon them may travel exceedingly fast -- much faster than an organization can be expected to update their anti-virus signatures and potentially faster than anti-virus companies can create and distribute signatures.

Use a Security Service like TruSecure which will provide, updated policies (updated at least quarterly for proven effectiveness), continuous alerts and information, emergency alerts and updates, and which will repeatedly measure and test the effectiveness of your sites implementation of these virus and numerous other security policies and practices. The service considers the malicious code risk as one of six risk categories (Electronic Risk (mostly hacking), Malicious Code Risk (mostly viruses), Privacy Risk, Downtime risk, Physical Risk, and Human Factors risk. Participation in the TruSecure program normally qualifies your organization TruSecure site certification that often satisfies due diligence and audit requirements. The process is continuous and constantly improving and it rapidly leads to effective security using the people and products already at your organization.

Submit Suggestions:

Please contribute your AV policy suggestions whether primary controls or supplemental / synergistic controls by sending e-mail to ‘avpolicy@icsa.net.’

ANNEX 1: Recommended settings for Microsoft Office programs to increase virus protection.

For Office 97 programs:
Word 97

Tools /Options /General:
- Do Check: [Macro virus protection]
- Do Not Check: [Mail as attachment]

Tools /Options / Save:
- Do Check: Prompt to save Normal template]
- Do not check: [Allow fast Saves]
- Do Configure: Save Word files as: Rich Text Format (*.rtf)

Excel 97

Tools /Options /General:
- Do Check: [Macro virus protection]

PowerPoint 97

Tools /Options /General:
- Do Check: [Macro virus protection]

Office 2000 Settings:

Word 2000

Tools | Macro | Security
- Security level = High (default is high)
- Trusted Sources = NO ONE
- Do not check “Trust all installed add-ins and templates.” (Default is checked)

Tools | Options | General:
- Do Not Check: Mail as attachment

Tools | Options | Save:
- Do Check: Prompt to save Normal template
- Do not check: Allow fast Save
- Do Configure: Save Word files as: Rich Text Format (*.rtf)

Excel 2000

Tools | Macro | Security
- Security level = High (default is high)
- Trusted Sources = NO ONE
- Do not check “Trust all installed add-ins and templates.” (Default is checked)

PowerPoint 2000

Tools | Macro | Security
- Security level = High – (Default may be medium)
- Trusted Sources = NO ONE
- Do not check “Trust all installed add-ins and templates.” (Default is checked.)

ANNEX 2: Recommended settings for Microsoft Outlook Security patches

Email Attachment Security Update for all versions of Outlook

This Update prevented users from automatically executing certain file types, instead forcing them to save these file types to disk.

Download and install the following depending on the version of Outlook which you use;

Outlook '97 http://officeupdate.microsoft.com/downloadDetails/O97attch.htm
Outlook '98 http://officeupdate.microsoft.com/downloadDetails/O98attch.htm
Outlook '2000 http://officeupdate.microsoft.com/2000/downloadDetails/O2Kattch.htm

The following url provides a fuller description of the Update. The Update prevents the automatic execution of .exe, .bat, .com, or .cmd file types.

http://support.microsoft.com/support/kb/articles/q235/3/09.asp

Microsoft Office SR-1

MS Office SR-1 provides further flexibility for Outlook 2000 than the previous versions. Included in SR-1 is an enhancement to the Email Attachment Security Update as described in;

http://support.microsoft.com/support/kb/articles/Q259/2/28.ASP

See the following for details.

http://officeupdate.microsoft.com/2000/downloadDetails/O2kSR1DDL.htm

ANNEX 3: File types

The list below contains a listing of file types that are recognized by default on machines with a complete installation of Office 2000. These may be automatically invoked when presented to the user as an attachment in Email.

??_
AD?
ADE
ADP
ASP
ASX
BAS
BAT
BIN
CDR
CER
CHM
CMD
COM
CPL
CRL
CRT
CSC
CSV
DER
DESKLINK
DEV
DIF
DL?
DO?
DOC
DOCHTML
DOT
DOTHTML
DQY
DSN
DUN
EML
EXE
FAV
GMS
GZ?
HLP
HT?
HT
HTA
HTM
HTML
HTT
HTW
IM?
INF
INI
INS
IQY
ISP
ITS
JOT
JS?
JSE
LNK
MAD
MAF
MAM
MAPIMAIL
MAQ
MAR
MAS
MAT
MAV
MAW
MD?
MDA
MDB
MDBHTML
MDE
MDT
MDW
MDZ
MSC
MHT
MHTML
MPP
MPT
MS?
MSI
MSP
MST
NFO
NMW
NWS
OBD
OBT
OCX
OLE
OQY
OSS
OV?
P10
P12
P7B
P7R
P7S
PBK
PFX
PKO
PCD
PIF
PL
PMA
PMC
POTHTML
POT
PP?
PPA
PPS
PPT
PPTHTML
PRF
PWZ
QDS
RNK
RQY
RTF
SC2
SCD
SCH
SCR
SCT
SHB
SHS
SLK
SMM
SNP
SPC
SST
STL
STM
SYSVB?
UDL
ULS
URL
VB?
VBE
VBS
VS?
WAB
WBK
WEBPNP
WHT
WIZ
WIZHTML
WPD
WS?
WSC
WSF
WSH
XLA
XLB
XLC
XLD
XLK
XLL
XLM
XLS
XLSHTML
XLT
XLTHTML
XLV
XLW
XML
XNK
XSL
XTP
XL?
ZAP