Revision	6/5/2004
Title	SecNet 5.0 Requirements
Copyright	Copyright 2004, Greene Software Systems Inc.
Confidentiality	The document is company confidential
Status	DRAFT for discussion purposes
Notes	Removed XP's security features from Redundant Security Applications' list

ID	Requirement	Additional notes
Platform Requirements		
ZPL001	The product shall operate on the Windows 98 SE	
ZPL002	The product shall operate on the Windows ME platform	
ZPL003	The product shall operate on the Windows 2000 platforms with SP3 and/or SP4	
ZPL004	The product shall operate on the Windows XP Home platform with SP1	
ZPL005	The product shall operate on the Windows XP Professional platform with SP1	
ZPL006	The product shall operate if applications listed in Co-existent Applications list are correctly installed, configured and operating on the end user's computer.	Applications of the Coexistent Applications list do not interfere with the operation of the product
~~ZPL007~~	~~Internet Explorer 5.0.1 SP2 or later must be installed on the end user's computer before the products security services may be activated.~~	This is not a requirement but more of a technological constraint. SecNet technology relies on IE browser functionality for many aspects like HTML rendering and Privacy Manager activity. This aspect will be documented as part of the System Requirements for SecNet.
Install Requirements		
ZIN001	The product shall install via an executable file	
ZIN002	The product shall create a Desktop shortcut	
ZIN003	The product shall create a program group	
ZIN004	Prior to completion of installation the product shall notify the user if any known 3d-party redundant security applications software is detected as listed in the Redundant Security Applications list	The product will notify the user of a if known 3d-party redundant security application software is detected
Activation Requirements		
ZAC001	The product shall attempt to activate security services as soon as an Internet connection is available after installation.	
ZAC002	Security services shall be activated if user authentication and authorization are successful.	
ZAC003	Security services shall not be available if the product is not activated.	The Activation is the process of authenticating the user and authorizing the security services he/she subscribed-to based on the authenticated user's account information. The activation involves the acquisition of the user's username and password credentials and it could occur with (user login) or without (e.g. via pre-dropped authentication cookie) the user's explicit intervention

ZAC004	The activated product shall run when an Internet Connection is not available	The Anti-Virus software will not receive the latest virus definitions in the absence of a connection.
SecNet Main Application Requirements		
ZFM001	The product shall place a icon in the system tray when started.	
ZFM002	The product shall minimize to the system tray when closed from the Desktop.	
Uninstall Requirements		
ZUN001	The product shall provide an uninstall utility	
ZUN002	When invoked the uninstall utility shall remove all installed artifacts except user profile-specific data files to recycle in future install	The process used follows Microsoft recommendations of keeping the files left behind under Application Data/Greene Software folder. They contain Security Services settings identification info for recycling in a future installation of SecNet Security Services. This is for the user's convenience.
Anti-Virus Requirements		
ZAV001	The Anti-Virus engine within the product passes ANTI-VIRUS DETECTION CERTIFICATION.	
ZAV002	The Anti-Virus service shall provide support to scan one or more sets of one or more drives, folders and files.	The AV scanner provides a tree view of the system drives, folders and files with section checkboxes next to each item in the tree. This allows maximum flexibility to chose groups of items or individual ones in a hierarchical manner. Also a right click menu feature allows such selection to be done directly on individual drives, folders or files outside of SecNet UI (e.g. Windows Explorer or Desktop)
ZAV003	The Anti-Virus service shall provide user-selectable options for automatic, manual, daily and weekly checks for virus definition file update.	
ZAV004	The Anti-Virus product shall provide a detailed report once the virus scan is ended.	
ZAV005	The Anti-Virus service provides scanning capability for POP3 email and their attachments	Note that encrypted ZIP files or password protected ZIP files will not be scanned.
ZAV006	The Anti-Virus product provides the capability of scanning non encrypted and non password protected zipped files	Encrypted and password-protected files cannot be scanned, otherwise there are non known file type restrictions. Everything getes scanned.
ZAV007	The Anti-Virus product displays the date and time of the last virus definition update.	

ZAV008	The Anti-Virus product displays the date and time of the last virus scan	
ZAV009	The Anti-Virus product provides the user with the capability to specify an action to be triggered upon virus detection. Possible actions are: 1- Attempt to disinfect the file 2- Delete the file 3- Report only	
ZAV010	The Anti-virus service shall provide a capability to define recurrent virus scan schedule item(s) by setting: - What file(s), folder(s) and drive(s) to scan. - The day(s) of the week to run the scan - The time-of-day to run the scan	
ZAV011	The Anti-Virus service provides the capability to enable or disable a real-time protection agains viruses	
ZAV012	The Anti-Virus service warns the user about infected files that are in use, recommends running a full scan and insures such files are tagged to be deleted after next reboot	
ZAV013	The Anti-Virus service provides a scan capability through a right-click menu feature	It can be used directly on individual drives, folders or files outside of SecNet UI (e.g. Windows Explorer or Desktop)
ZAV014	The Anti-Virus service shall maintain a detailed log of last scan results detailing boot sector, drives, folders and files scans	
Firewall Requirements		
ZFW001	The firewall service warns users when unauthorized programs attempt to send information to remote machines over the internet.	
ZFW002	The firewall service provides a capability which allows user's to disable the firewall functionality.	
ZFW003	The firewall service provides a capability which allows user's to allow a program to access the internet	
ZFW004	The firewall service provides a capability which allows user's to block a program from accessing the internet.	
ZFW005	The firewall service provides a capability which allows user's to add programs for which internet access rules can be defined.	
ZFW006	The firewall service provides a capability which allows user's to remove programs for which internet access rules can be defined.	
ZFW007	The firewall service provides a capability which allows user's to manage program rules by setting options to Allow, Block or Disable a rule for a program.	

ZFW008	The firewall service provides a capability which allows user's to view a list of programs with active connections.	
ZFW009	The firewall service provides a capability which allows user's to view a detailed log of blocked connections.	
Anti-Spyware Requirements		
ZAS001	The Anti-Spyware product provides the user with the capability to delete all detected spyware from the users machine	
ZAS002	The Anti-Spyware product provides a real-time scan capability that frequently scans for the following: 1- Spyware Cookies every 4 minutes 2- Spyware Registry Keys every 6 minutes 3- In-memory Spyware Programs every 2 minutes	
ZAS003	The Anti-Spyware service shall provide a capability to establish a scan schedule.	
ZAS004	The Anti-Spyware service shall provide user-selectable options for automatic, manual, daily and weekly checks for anti-spyware definition file update.	
ZAS005	The Anti-Spyware product displays the date and time of the last Spyware definition update.	
ZAS006	The Anti-Spyware service shall maintain a log of deleted spyware and a list of non-deleted spyware	
Popup/Ad Blocker Requirements (only available for IE)		
ZPB001	The Pop-up Blocker provides the capability to block Internet Explorer-generated pop-up windows	
ZPB002	The Pop-up Blocker provides the capability to block web browser HTTP ads.	
ZPB004	The user must be able to disable the Pop-up Blocker feature.	
ZPB005	The user must be able to disable the Ad Blocker feature	
ZPB006	The Ad Blocker service provides the capability to manually update the Blocked Ads List	
ZPB007	The Ad Blocker service provides the capability for adding an address to the Blocked Ads List	
ZPB008	The Popup Blocker service shall maintain a log of blocked popups	
Privacy Manager Requirements		
ZPM001	The Privacy Manager shall provide the capability to detect user-listed keywords communicated through applications using HTTP and SMTP protocols (I.E. SSN and credit card)	Scenarios with clean now
ZPM002	The Privacy Manager shall provide the capability to detect user-listed keywords communicated through IRC chat applications.	

ZPM003	The Privacy Manager product provides the capability for the user to decide whether to allow or block detected communication of the user-listed information.	
ZPM004	The Privacy Manager shall provide the capability add IE browser cookies to a Trusted Web Sites List	
ZPM005	The Privacy Manager product must provide the capability to remove IE browser history	
ZPM006	The Privacy Manager product must provide the capability to clean IE browser cache.	
ZPM007	The Privacy Manager product must provide the capability to remove IE browser cookies	
ZPM008	The Privacy Manager should provide the capability to add keywords to the keyword list.	
ZPM009	The Privacy Manager should provide the capability to delete keywords from the keyword list.	
Parental Control Requirements		
ZPC001	The Parental Control service must provide out-of-the-box filtering capability of remote, non-cached HTTP communication	The filtering technology used applies regardless whether access to sites occurs via domain names or IP addresses: An AI engine analyses the Web page content on the fly decides of appropriateness or not. This technology renders the IP vs. domain name access methods irrelevant
ZPC002	The Parental Control service must provide the ability to deny new Internet connections to a list of restricted programs	
ZPC003	The Parental Control service must provide the ability to add new programs to the list of restricted programs	
ZPC004	The Parental Control service must provide the capability to remove a program from the list of restricted programs	
ZPC005	The user must be able to disable the parental control product.	
ZPC006	The user must be able to set a password for the parental control product.	
ZPC007	The user must be able to add sites to the list of sites to block from browsing.	This applies for both individual URLs or domain level ones
ZPC008	The user must be able to remove sites from the list of sites to block from browsing	This applies for both individual URLs or domain level ones
ZPC009	The user must be able to add sites to the list of sites to allow for browsing.	This applies for both individual URLs or domain level ones
ZPC010	The user must be able to remove sites from the list of sites to allow for browsing.	This applies for both individual URLs or domain level ones
ZPC009	The Parental Control service shall maintain a log of blocked sites	
Performance Requirements		

ZPR001	The Windows Benchmark Tool measure on a recommended system with a freshly installed operating environment varies by less than 30% between the case of SecNet not installed and SecNet installed with only Firewall services enabled.	Same normal internet traffic is required each time the Windows Benchmark Tool is run, Windows XP Home platform.
ZPR002	The Windows Benchmark Tool measure on a recommended system with a freshly installed operating environment varies by less than 30% between the case of SecNet not installed and SecNet installed with only Antivirus services enabled.	Real time scanning is enabled but no manual scan is operating. Same normal internet traffic is required each time the Windows Benchmark Tool is run, Windows XP Home platform.

Redundant Security Applications List

ID	Requirement
SS	Security Suites/Bundles
ZIDSS001	Norton Internet Security 2004
ZIDSS002	McAfee Internet Security Suite 6.0
AV	Antivirus
ZIDAV001	(Norton AV 2004, Paid)
ZIDAV003	(McAfee Virus Scan, Paid)
ZIDAV005	(Panda Titanium 2004, Paid)
ZIDAV007	(AVG Antivirus Professional v7, Paid)
ZIDAV009	Norton 2001
FW	Firewall
ZIDFW001	(Norton Personal Firewall 2004)
ZIDFW003	(McAfee Personal Firewall Plus v5.0)
ZIDFW004	(Zone Labs Firewall 4.x, Paid)
ZIDFW006	(Blacke Ice Firewall 3.6)

Coexistant Internet Applications List

ID	Application
EM	Email
ZCEEM001	NS 7
ZCEEM002	Eudora 5.21
ZCEEM003	OE 6
ZCEEM004	Outlook 2003
ZCEEM005	Eudora 6
ZCEEM006	Outlook 97
ZCEEM007	OE 5
ZCEEM008	Outlook Express XP
WM	Web Mail
ZCEWM001	AOL9
ZCEWM002	Yahoo
ZCEWM003	Hotmail
ZCEWM004	OWA
ZCEWM005	AOL7
ZCEWM006	AOL8
ZCEWM007	Lepton Webmail
CH	Chat
ZCECH001	Yahoo
ZCECH002	AOL IM
ZCECH003	ICQ
ZCECH004	MSN
ZCECH005	NetMeeting
ZCECH006	Trillian
SH	Sharing
ZCESH001	Kazaa
ZCESH002	Morpheus
ZCESH003	WinMX
ZCESH004	Imesh
DA	Desktop Applications
ZCEDA001	MS-Office
WB	Web Browser
ZCEWB001	IE5 sp2
ZCEWB002	IE 6
ZCEWB003	NS Nav 6
ZCEWB004	MSN8
ZCEWB005	AOL9
ZCEWB006	Opera
GA	Games
ZCEGA001	Everquest
ZCEGA002	Quake
ZCEGA003	Halflife
ZCEGA004	Starwars Galaxies
ZCEGA005	Diablo
PO	Popular
ZCEPO001	Ad-Aware
ZCEPO002	Limewire
ZCEPO003	Realplayer
ZCEPO004	eMule

ZCEPO005	WS-FTP
ZCEPO006	Windows Media Player
ZCEPO007	Freeware Netzero Internet Remote Dialup

Product	SecNet 5.0							
Recommended System	IBM Compatible	PII	300 MHz	128 MB RAM	WINDOW XP	WINDOWS 2000	WINDOWS 98 SE	WINDOWS ME
Windows Benchmark Tool	A tool which provides a measure of the operational performance of a windows based computer.							
ANTIVIRUS Certification	Third party lab test of ANTIVIRUS Capabilities of the product							