Xerox® Products and Anti-Virus Software

Version 5.2

November 2015

Document Version: 5.2 (November 2015).

Introduction

Purpose and Audience

This document was created in response to customer inquiries regarding Xerox position on the use of anti-virus software on Xerox® products. This document is meant to clarify the Xerox position and is for informational purposes only; it is not meant as an endorsement of any anti-virus software application.

The primary audience of this document is Xerox customers and analysts.

Xerox Position with Respect to Anti-Virus Software

Anti-virus software may not be supported by all equipment and/or configurations. Use or application of anti-virus software is at the customer's sole discretion and risk and should only be undertaken after independent review. Xerox shall not be liable for damages of any kind attributable to the use of anti-virus software.

The table below lists various products and their positions with respect to anti-virus software. The table will be updated with additional product information as it becomes available.

Contact

For additional information or clarification on any of the product information given here, contact Xerox support.

Production	Position with respect to Anti-Virus Software	Additional Information
CSX2000 (NT based System)	Xerox and Creo® understand that customers with CSX2000 products connected to Xerox® print engines are concerned about computer viruses. Xerox and Creo do not provide antivirus software	If a customer suspects there is a virus on a CSX2000, formatting and reloading the operating system and the CSX2000 application can remove the virus. Customers may install McAfee® VirusScan® software version 4.5 or 4.5.1 on the CSX2000 to minimize the risk of computer damage. Creo and Xerox have tested compatibility of the anti-virus software with the DFE software to ensure to there are no issues. Xerox sales and service personnel should refer to customer bulletin #39, which describes the use of virus protection software on a CSX2000 DFE. **NOTE:** Customers who wish to install McAfee VirusScan on their CSX2000 are advised that enabling this software to run in auto-protect mode will result in decreased system productivity and performance. To limit degradation of performance, it is recommended to avoid using auto-scan mode, and to activate the anti-virus software only when the CSX2000 Color Server application, is closed. Before installing the CSX2000 software, ensure that anti-virus application and all other **For optimum performance:** We recommend that McAfee VirusScan software be configured exactly as described in the CSX2000 Technical Manual applications are closed.
CXP3535 (Win 2000 Professional)	Xerox and Creo understand that customers with CXP3535 products connected to Xerox® print engines are concerned about computer viruses. Xerox and Creo do not provide antivirus software.	If a customer suspects there is a virus on a CXP3535, formatting and reloading the operating system and the CXP3535 application can remove the virus. Customers may install McAfee VirusScan software version 4.5 or 4.5.1 on the CXP3535 to minimize the risk of computer damage. Creo and Xerox have tested compatibility of the anti-virus software with the DFE software to ensure to there are no issues. NOTE: Customers who wish to install McAfee VirusScan on their CXP3535 are advised that enabling this software to run in auto-protect mode will result in decreased system productivity and performance. To limit degradation of performance, it is recommended to avoid using auto-scan mode, and to activate the anti-virus software only when the CXP3535 Color Server application, is closed. Before installing the CXP3535 software, ensure that anti-virus application and all other applications are closed. For optimum performance: We recommend that McAfee VirusScan software be configured exactly as described in the CXP3535 Technical Manual.
CXP5000 CXP6000 (Win 2000 Professional)	Xerox and Creo understand that customers with CXP6000 products connected to Xerox® print engines are concerned about computer viruses. Xerox and Creo do	If a customer suspects there is a virus on a CXP6000, formatting and reloading the operating system and the CXP6000 application can remove the virus. Customers may install McAfee VirusScan software version 8.0 on the CXP6000 to minimize the risk of computer damage. Creo and Xerox have tested compatibility of the anti-virus software with the DFE software to ensure to there are no issues. NOTE: Customers who wish to install McAfee VirusScan on their CXP6000 are advised that enabling this software to run in

Production	Position with respect to Anti-Virus Software	Additional Information
	not provide antivirus software.	auto-protect mode will result in decreased system productivity and performance. To limit degradation of performance, it is recommended to avoid using auto-scan mode, and to activate the anti-virus software only when the CXP6000 Color Server application, is closed. Before installing the CXP6000 software, ensure that anti-virus application and all other applications are closed. For optimum performance: We recommend that McAfee VirusScan software be configured exactly as described in the CXP6000 Technical Manual.
CXP8000 CX8000AP CX8002 CXP3535e CX250 CX700 (Win XP Professional)	Xerox and Creo understand that customers with CXP8000 products connected to Xerox® print engines are concerned about computer viruses. Xerox and Creo do not provide antivirus software.	If a customer suspects there is a virus on a CXP8000, formatting and reloading the operating system and the CXP8000 application can remove the virus. Customers may install McAfee VirusScan 8.0 for Windows XP Professional server Anti-virus software on the CXP8000 to minimize the risk of computer damage. Creo and Xerox have tested compatibility of the anti-virus software with the DFE software to ensure to there are no issues. NOTE: Customers who wish to install McAfee VirusScan on their CXP8000 are advised that enabling this software to run in auto-protect mode will result in decreased system productivity and performance. To limit degradation of performance, it is recommended to avoid using auto-scan mode, and to activate the anti-virus software only when the CXP8000 Color Server application, is closed. Before installing the CXP8000 software, ensure that anti-virus application and all other applications are closed. For optimum performance: We recommend that McAfee VirusScan software be configured exactly as described in the CXP8000 Technical Manual, Customer Documentation, and Customer Release Notes.
DocuColor®1632/2240 Printer/Copier	The product does not allow for customer installation of anti-virus software	The operating system on the DocuColor 1632 and 2240 is a dedicated, proprietary operating system, and therefore does not have all the functionality of a complete operating system. The products were not designed to accept applications such as virus protection software as part of their operational model. (This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.)
DocuColor 3535 Multifunction printer DocuColor 240/250 Printer/Copier Bustled Network Controller (Linux-based systems)	Xerox and Electronics for Imaging, Inc. (EFI®) understands that customers with Fiery® products connected to Xerox® print engines are concerned about computer viruses.	The operating system is a dedicated operating system, and therefore does not have all the functionality of a complete operating system. The Bustled Controller was not designed to accept applications such as virus protection software as part of their operational model. (This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance.)

Production	Position with respect to Anti-Virus Software	Additional Information
	The product does not allow for customer installation of antivirus software. Refer to the Fiery Security White Paper for details. Please contact your Xerox or EFI support representative to obtain the white paper.	
DocuPrint® N Network Laser Printer Series products	Anti-virus software is not needed with DocuPrint N Series products.	DocuPrint N Series products are embedded products that do not run any software that was not installed at the factory; they do not run Windows, Apple, or Unix/Linux software. Anti-virus software is therefore not needed with DocuPrint N Series products. DocuPrint N Series products include application and/or driver software that can be loaded on host machines (e.g., Windows, Mac, and Unix/Linux). These applications and drivers are compatible with anti-virus software.
DocuSP®/FreeFlow® Print Server based products	While installing anti-virus software is not prohibited, Xerox has not tested anti-virus applications for the Sun/Solaris Operating System with the DocuSP and FreeFlow Print Server platforms and cannot comment on their effectiveness or possible impact to the productivity and reliability of these Production Printers.	Anti-virus software products that are available for Solaris Operating System focus on detecting viruses that are received via email. Starting with DocuSP 3.8 and up, and FreeFlow Print Server 6.0 and up, the Email Receive service is disabled by default. Therefore, software that protects against incoming mail viruses is not required. To effectively stop the spread of virus software that might have been introduced into FFPS via removable media or USB drives, the SA can disable these ports and block email from being sent by FFPS
Extended Connectivity Print Job Manager EC-PJM	Xerox strongly recommends customer installation and use of anti-virus software.	Xerox takes special precautions to ensure that EC-PJM is shipped free from computer virus contamination. Xerox recommends that customers invest in a virus detection software application to continue to protect their EC-PJM system from viruses. Computer viruses are best detected by virus detection and control application software that is accepted by the PC industry. To ensure maximum protection from new viruses, customers should update or upgrade their virus detection software regularly.

Production	Position with respect to Anti-Virus Software	Additional Information
		Xerox also strongly recommends that customers incorporate the following guidelines into their work practices in order to help keep their EC-PJM systems free of viruses: GUIDELINES: • On a regular basis (weekly), run virus protection software on all EC-PJM servers. • If a virus is detected on an EC-PJM server, do not remove the virus. Instead, cancel the virus detection application, and back up important user files, including pending or saved documents. Rerun the virus protection software, and repair/remove any detected viruses.

Production	Position with respect to Anti-Virus Software	Additional Information
EX12/X12/XP12/X40 Fiery Families (NT® based systems)	Xerox and Electronics for Imaging, Inc. (EFI) understands that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However, both companies have tested compatibility and have seen no adverse effects when configured as described. Refer to the Fiery Security White Paper for details. Please contact your Xerox or EFI support representative to obtain the white paper.	If a customer suspects there is a virus on a Fiery product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox validated server systems with Symantec Norton Antivirus. Similar products from McAfee and TrendMicro® are also compatible with the Fiery servers when used as the guideline described below. However, issue resolution is not guaranteed. In testing to date, EFI and Xerox have not found any application conflicts. NOTES: 1. Installing anti-virus software on a Fiery without a FACI kit is not supported. However, for such cases, it is possible to launch anti-virus software on a remote PC and scan a shared hard drive of a Fiery. Refer to the anti-virus software documentation to scan the Fiery from a remote PC. 2. Customers who wish to install Antivirus on their Fiery Family product are advised that enabling this software to run in auto-protect mode will result in decreased system productivity and performance. To resolve performance degradation, it is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 3. The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes: • Removable media • Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job.

Production	Position with respect to Anti-Virus Software	Additional Information
EX12 EX3535 Phaser® EX7750 X12 XP12 (XPe® Based Systems)	Xerox and Electronics for Imaging, Inc. (EFI) understands that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However, both companies have tested compatibility and have seen no adverse effects when configured as described. Refer to the Fiery Security White Paper for details. Please contact your Xerox or EFI support representative to obtain the white paper.	If a customer suspects there is a virus on a Fiery product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox validated server systems with McAfee. Similar products from Symantec and TrendMicro are also compatible with the Fiery servers when used as the guideline described below. However, issue resolution is not guaranteed. In testing to date, EFI and Xerox have not found any application conflicts. NOTES: 1. Installing anti-virus software on a Fiery without a FACI kit is now supported with Windows Remote Desktop tool. This is enabled on the EX3535 using Fiery patch 1-E4VH1. This new workflow is described in detailed documentation available at www.xerox.com. 2. Customers who wish to install Norton Antivirus on their Fiery Family product are advised that enabling this software to run in auto-protect mode is not supported. It is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 3. The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes: • Removable media • Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job.

Production	Position with respect to Anti-Virus Software	Additional Information
EX2000 Series/EXP6000 (NT® Based Systems)	Xerox and Electronics for Imaging, Inc. (EFI) understands that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However both companies have tested compatibility and have seen no adverse effects when configured as described. Refer to the Fiery Security White Paper for details. Please contact your Xerox or EFI support representative to obtain the white paper.	If a customer suspects there is a virus on a Fiery product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox validated server systems with Symantec Norton Antivirus. Similar products from McAfee and TrendMicro are also compatible with the Fiery servers when used as the guideline described below. However, issue resolution is not guaranteed. In testing to date, EFI and Xerox have not found any application conflicts. NOTES: 1. Customers who wish to install Antivirus on their Fiery Family product are advised that enabling this software to run in auto-protect mode is not supported. It is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 2. The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes: • Removable media • Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job.
EX2101 EXP250 EX8000AP EX8002 (XPe Based Systems)	Xerox and Electronics for Imaging, Inc. (EFI) understand that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However, EFI has tested compatibility and has seen no adverse effects when configured as described. Refer to the Fiery Security White Paper for details. Please	If a customer suspects there is a virus on a Fiery product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox validated server systems with TrendMicro. Similar products from Symantec and McAfee are also compatible with the Fiery servers when used as the guideline described below. However, issue resolution is not guaranteed. In testing to date, EFI has not found any application conflicts. NOTES: 1. Customers who wish to install Norton Antivirus on their Fiery Family product are advised that enabling this software to run in auto-protect mode is not supported. It is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 2. The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes:

	contact your Xerox or EFI support representative to obtain the white paper.	• Removable media • Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job.

Production	Position with respect to Anti-Virus Software	Additional Information
EXP5000 EXP6000 EXP8000 (XPe Based Systems)	Xerox and Electronics for Imaging, Inc. (EFI) understands that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However, both companies have tested compatibility and have seen no adverse effects when configured as described. Refer to the Fiery Security White Paper for details. Please contact your Xerox or EFI support representative to obtain the white paper.	If a customer suspects there is a virus on a Fiery product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox validated server systems with McAfee. Similar products from Symantec and TrendMicro are also compatible with the Fiery servers when used as the guideline described below. However, issue resolution is not guaranteed. In testing to date, EFI and Xerox have not found any application conflicts. NOTES: 1. Customers who wish to install Antivirus on their Fiery Family product are advised that enabling this software to run in auto-protect mode is not supported. It is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 2. The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes: • Removable media • Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job.
FreeFlow® Applications FreeFlow Makeready FreeFlow Process Manager FreeFlow Express to Print FreeFlow Output Manager FreeFlow Web Services	Xerox strongly recommends customer installation and use of anti-virus software.	Xerox takes special precautions to ensure its software is shipped free from computer virus contamination. It is strongly recommended that you invest in a virus detection software application to protect your system from viruses. Computer viruses are best detected by virus detection and control application software that is accepted by the PC industry. Some of the virus detection and control applications available to and widely-used by the PC industry include: • Norton® Anti-Virus™ by Symantec™ • McAfee VirusScan by Network Associates, Inc. NOTES: 1. To ensure maximum protection from new viruses, update or upgrade your virus detection software frequently. It is strongly recommended that you follow these guidelines to keep your system decontaminated: • On a regular basis (at least weekly), run virus detection

		software on all systems. • In the event you find a virus on a system, delete the infected file using Document Library. Then, recover the file via restore. 2. This is to protect your data in the event of corruption during the course of the virus removal.

Production	Position with respect to Anti-Virus Software	Additional Information
iGen®3 with Creo Color Server	McAfee anti-virus software can be used. There will be some negative effect on performance that can be minimized by following the configuration/setup instruction in the Install Guide.	See the Installation Guide for more details.
iGen3 with EFI Color Server	There is no recommended virus protection software package.	
Phaser products	Anti-virus software is not needed with Phaser products.	Phaser products are embedded products that do not run any software that was not installed at the factory; they do not run Windows, Apple, or Unix/Linux software. Anti-virus software is therefore not needed with Phaser products. Phaser products include application and/or driver software that can be loaded on host machines (e.g., Windows, Mac, and Unix/Linux). These applications and drivers are compatible with anti-virus software.
Splash® G-Series products	Xerox and Electronics for Imaging, Inc. (EFI) understands that customers with Fiery products connected to Xerox® print engines are concerned about computer viruses. Xerox and EFI do not provide antivirus software. However, both companies have tested compatibility and have seen no adverse effects when configured as described. Please contact your Xerox or EFI support	If a customer suspects there is a virus on a Splash product, the recommended course of action is to remove the virus by formatting and reloading system software. An alternative course of action to address the concern about viruses is to run third-party anti-virus applications directly on the Fiery servers themselves. Although this is not the recommended course of action, EFI and Xerox will at this time support server systems with Norton Antivirus. However, issue resolution is not guaranteed. In testing to date, EFI and Xerox have not found any application conflicts. NOTES: 1. Customers who wish to install Norton Antivirus 9.X on their Splash Family product are advised that enabling this software to run in auto-protect mode is not supported. It is recommended that customers avoid the auto scan mode and activate the anti-virus software with all other applications closed and the server idle. 2. The anti-virus software should be configured to scan for files coming into the Splash outside of the normal print stream. This includes: • Removable media • Files copied to the Splash from a shared network directory The anti-virus software can also be configured to scan all files on the

	representative to obtain the product specific white paper.	Splash when the Splash is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Splash is idle and not receiving or acting upon a job.

Production	Position with respect to Anti-Virus Software	Additional Information
WorkCentre®/ WorkCentre Pro® Document Centre® products	Document Centre, WorkCentre and WorkCentre Pro products do not allow for customer installation of anti-virus software.	The operating systems on the WorkCentre products are either proprietary or embedded inside the product. All access to the OS is mediated by the application software, so there is no way for an attacker to access these operating systems via the network and login as one could with Unix or Windows, for example. The products are designed to prevent the loading of any third-party applications as part of their operational model, this includes anti-virus software. This was done intentionally to help prevent the loading of potentially malicious software on the units, as well as to control the impact adding such applications would have on a system's operation and performance. Moreover, anti-virus vendors do not make virus protection software that is specific to Xerox® embedded products.
WorkCentre 7328/7335/7345/7346 Color Multifunction printer 7425/7428/7435 Color Multifunction printer 7755/7765/7775 Color Multifunction printer With Fiery Digital Front Ends	WorkCentre and WorkCentre Pro products with EFI Fiery digital front ends that are equipped with FACI kits do allow for direct customer installation of anti-virus software	Windows anti-virus software Administrators can install anti-virus software on a Fiery with FACI kits. A local GUI is required for proper configuration of anti-virus software. Anti-virus software is most useful in a local GUI configuration, where users have the potential to infect the Fiery with a virus through standard Windows actions. For a Fiery without a FACI kit, it is still possible to launch anti-virus software on a remote PC and scan a shared hard drive of a Fiery, EFI supports this configuration/ workflow. However, EFI suggests the Fiery administrator work directly with the anti-virus software manufacturer for support of this operation. EFI tests Fiery products with McAfee VirusScan software; similar products from Symantec and TrendMicro are also compatible with the Fiery when used as described above. Anti-Virus Software Configuration The anti-virus software should be configured to scan for files coming into the Fiery outside of the normal print stream. This includes: Removable media Files copied to the Fiery from a shared network directory The anti-virus software can also be configured to scan all files on the Fiery when the Fiery is not planned for use for an extended period of time. The administrator should only run the anti-virus software manually when the Fiery is idle and not receiving or acting upon a job. Non-FACI Systems For non-FACI based Fiery Systems, because the system is running on Microsoft OS, EFI recognizes that the Fiery must still meet the customer's company anti-virus standards. EFI has developed a patch that enables remote desktop. With this patch installed and remote desktop enabled, the administrator will be able to manage the NON-FACI system using remote desktop – and install the appropriate anti-virus software required by the company.

Production	Position with respect to Anti-Virus Software	Additional Information
Xerox® 1010 Digital Copier Xerox® 1010 ST Copier/Printer Xerox® 2101 Digital Copier Xerox® 2101 ST Copier/Printer (Copy Server ONLY)	Xerox Corporation understands that customers with Xerox® 1010 or Xerox® 2101 Digital Copier are concerned about computer viruses. Xerox does not provide antivirus software. However, Xerox has tested the compatibility with the digital copier and has seen no adverse effects when configured as described.	To address concerns about viruses, customers can install and run a third-party anti-virus application directly on the Xerox® 1010 or Xerox® 2101 copy servers themselves. Although this is not the recommended course of action, Xerox has validated the copy server systems with Symantec® Norton Antivirus, VirusScan®, and VirusBuster2003®. These third party applications are compatible with the Xerox® 1010 or Xerox® 2101 copy servers when installed exactly as described in "Xerox® 1010 / Xerox® 2101 Digital Copier (Copy Server) Anti-Virus installation - How to Install an Anti-virus Software Program" which can be found in Appendix A of this document. NOTES: 1. The Anti-Virus install procedure is ONLY for the copier portion. 2. The installation on the copy server is separate from the DFE. The customer must insure they have the required number of licenses if they wish have anti-virus s/w on both the DFE and the copier. 3. For the DFEs please refer to the Anti-Virus statements contained in the Fiery Security White Paper. Please contact your Xerox or EFI support representative to obtain the white paper.

Appendix A

Xerox® 1010 / Xerox® 2101 Digital Copier (Copy Server) Anti-Virus Installation: How to Install an Anti-virus Software Program

The Setting of Each Anti-virus Software Program

When installing an anti-virus software program in NEX Extension, all the options indicated below must be made "Invalid." (This setting can be changed during or after installing.)

The name of each option in each anti-virus software program is indicated below.

Option	Norton Antivirus 2002	VirusScan Ver4.51SP !	VirusBuster2003
Automatic Update of Pattern File	Live Update	Automatic Upgrade of DAT	
Automatic Execution of Scheduled Virus Scan	Startup Scan Scheduled Scan	My Computer Scan C Drive Scan Scheduled Scan	Task Search
Automatic Monitoring Program	Real Time Protection	V Shield (System scan)	Real Time Search
Others			Mail Search, WebTrap, URL Filter, Personal Fire Wall

Preparation

1. Connect the keyboard and mouse.
2. Press "Interrupt" + "Reset" + "Meter Check" buttons together. (Interrupt LED will blink every second.)
3. Press "Reset" + "Password" buttons together. (Interrupt LED will blink every 0.5 second.)

   By following the above steps, the keyboard and mouse will be usable.

Procedures for Installing

1. Turn on the power of NEX Extension.
2. When the blue screen (figure right) is displayed at the start up screen of WindowsNT4.0, press the “Shift” key. The “Shift” key can be pressed anytime as long as the blue screen is displayed. Keep pressing the “Shift” key until the log on dialog appears.
3. After confirming that the user name is (XXX) and the password is (XXX), log on (press OK button) while pressing the “Shift” key again.
4. Release the “Shift” key approximately 20 seconds after the start menu is displayed.
5. Icons such as “My Computer” will not appear on the desktop. Start-up Windows NT Explorer (“Start” → “Program” → “Windows NT Explorer”) and install each software program. For installment procedures, see the Readme section in each patch or see anti-virus software program manuals.
6. When installing the anti-virus software program, all the options that reside in the main memory, such as “Automatic Update of Pattern File,” “Automatic Monitoring Program,” and “Automatic Execution of Scheduled Virus Scan,” must be made “Invalid.”
7. After installing, restart Windows NT4.0.

How to Run Anti-virus Software Program (The options are to be made invalid after updating and scanning.)

1. Follow steps 1 through 4 in the above “Procedures for Installing.”
2. Icons such as “My Computer” will not appear on the desktop. Run each anti-virus software program from the “Start” menu.
3. Following the anti-virus software program manual, update the pattern file or carry out virus scan.
4. After completing the above steps, restart WindowsNT4.0.