

FREE Advisory Report:

Critical Steps Every Small Business Owner Must Take To Protect Themselves From Inappropriate Employee Activities Online

- Does your computer network run slow, act funny, or crash unexpectedly?
- Do you constantly get hammered by pop-up ads that come from nowhere and interfere with using your computer?
- Are you getting tons of spam from unknown senders?
- Do you see or suspect that employee productivity drops significantly when you or your managers are not in the office?

If so, then the computers on your network are probably infected with malicious programs that could end up destroying your files, stealing your company's confidential and financial information, and rendering your computer useless. Chances are most of these programs came directly from your own employees who were surfing, shopping or visiting their facebook account while at work.

Don't Be A Victim To Employee Induced Online Crime!

Employees, even your most trusted ones, are constantly surfing the internet and taking care of personal business while at work. Meanwhile, these activities are damaging your network with viruses, spyware, and security holes. If you want to automatically stop these activities, increase employee productivity, and secure your network, read this guide to discover:

- ✓ Computer scams, threats, and rip-offs that you **MUST** be aware of.
- ✓ Surefire signs that you are infected with spyware, malware, and viruses.
- ✓ Sneaky, underhanded ways cyber criminals access your computer, and how you can stop them dead in their tracks.
- ✓ The absolute worst type of program to install for your network's health; if you or your employees go to these sites and indulge in these seemingly innocent activities then you're practically guaranteed to get infected with vicious spyware and destructive viruses.
- ✓ The single biggest cause of expensive computer repairs – and how to avoid it.
- ✓ 7 simple steps to keep your network safe from pop-ups, viruses, spyware, malware, inappropriate employee online activities and expensive computer repair bills.

Provided as an educational service by:

Jennifer L. Holmes

MIS Solutions, Inc.

4485 Tench Rd, Suite 440, Suwanee, GA 30024

Phone: 770-945-5487 Fax: 770-932-4287

www.mis-solutions.com

Dear Colleague:

If you are a business owner with a computer network connected to the Internet, then it is only a matter of time before you fall victim to a malicious spyware program, virus, worm, or hacker. Every day we get customers calling our office who are experiencing computer problems due to these threats – which are introduced by employees who are surfing, emailing and shopping online while at work. The problem *is only getting worse*.

What is even more frustrating is that many of these clients call back a few days or weeks later with the EXACT same problems and end up having to spend ANOTHER hefty fee for restoring their computer network back to normal. Unless you learn how to secure your network from cyber criminals and stop your employees from using your company's email and internet inappropriately, you will constantly fall victim to these threats and end up spending hundreds – possibly even thousands – of dollars to get your computer network running normal again.

With the tight economy, we have seen a sharp increase in the number of businesses falling victim to these attacks and that is why I decided to write this report. I wanted to arm my clients with the facts so they could avoid problems and expensive repair bills.

The information in this Report will not only educate you as to WHY you are experiencing these problems, but also what you **must** do now to guard against the unethical actions of these cybercriminals and your own employees inappropriate or innocent online activities at work.

Three Most Common and Dangerous Threats You Must Be Aware Of

One of the most dangerous aspects of online threats is their ability to cloak their existence. Hackers and the authors of malicious spyware and malware programs go to great lengths to create programs that are difficult to identify and remove. They are also highly experienced at finding tiny, overlooked loopholes in your security to access and infect your network undetected.

That means a malicious program can be downloaded and doing its dirty work on your network long before you are aware of it. Below are the three most common threats you'll need to guard against with a brief explanation of what they are:

Spyware: Spyware is Internet jargon for hidden programs advertisers install on your PC without your permission to spy on you, gather information, and report this information about you and your online activities to some outside person.

Spyware is NOT harmless; it can be responsible for delivering a boatload of spam, altering your web browser, slowing down your PC, and serving up a bounty of pop-up ads. In some of the more extreme cases, spyware can also steal your identity, passwords, e-mail address book, and even use your PC for illegal activities.

Most spyware finds its way onto your computer network via file downloads including free programs, music files, and screen savers. While you *think* you are only downloading a legitimate program to add emoticons to your e-mails, you are unknowingly also downloading a heaping spoonful of spyware programs. All it takes is one employee downloading a questionable file to infect your entire network.

Spyware piggybacks the download and runs undetected in the background collecting information about you and sending it back to its originator until it is removed. Although spyware has malicious components, it is not illegal, and it is not considered a virus because it doesn't replicate itself or destroy data.

Malware: Malware is short for **malicious software** and represents all programs, viruses, Trojans, and worms that have malicious intent to damage or disrupt a system. Malware is harder to remove and will fight back when you try to clean it from your system. In some extreme cases, we have had to completely wipe out all of the information on the computers' hard disk and start with a complete re-install of the operating system.

Among other things, a malware infection can corrupt your files, alter or delete data, distribute confidential information such as bank accounts, credit card numbers, and other personal data; it can also disable hardware, prevent you from using your computer, and cause an entire network to crash. Malware is designed to replicate itself from one computer to the next either through a network connection or via your e-mail account without your knowledge or consent.

Hackers: Hackers are computer programmers turned evil. They are the people who design the spyware and malware programs that attack your computer.

Some of them have criminal intent and use these programs to steal money from individuals and companies. Some have a grudge against the big software vendors (like Microsoft) and seek to harm them by attacking their customers (you). Others do it purely for fun. Whatever the reason, hackers are getting more intelligent and sophisticated in their ability to access computer systems and networks.

Surefire Signs That You Are Infected With Spyware, Malware, and Viruses from Inappropriate Employee Online Activities Such As Surfing, Playing Games, Downloading Inappropriate Content and Checking Personal Email

Since most malicious programs are designed to hide themselves, detecting their existence is not always easy. However, there are a few surefire signs that you have been infected:

- You start getting swamped with pop-up ads that seem to come from nowhere and constantly interrupt your use of the computer.
- Your computer is unstable, sluggish, locks up, or crashes frequently.
- Your web browser's home page changes on it's own and you cannot modify the settings.
- You may also see toolbars on your web browser that you did not set up.
- You get a second or third web browser popping up behind your main browser that you didn't open or request.
- Mysterious files suddenly start appearing.
- Your CD drawer starts opening and closing by itself.
- You get constant runtime errors in MS Outlook/Outlook Express.
- You find emails in your "Sent Items" folder that you didn't send.
- Some of your files are moved or deleted or the icons on your desktop or toolbars are blank or missing.

If you are experiencing one or more of the above when using your computer, you are infected and should seek help from a senior computer technician. Before I talk about getting rid of it, let me share with you 4 costly misconceptions about spyware, malware, hackers, and other threats that you will also need to know...

The Four Most Costly Misconceptions About Spyware, Malware, And Other Computer Threats

#1: Spyware and Malware is easy to remove.

Some spyware and malware CAN be easily removed using a program such as Spybot's Search & Destroy (you can download it for free at: www.safer-network.org) or Ad-Aware (you can download it at www.lavasoftusa.com/support/download).

However, not all malicious programs can be removed – or even detected – using the above software. Many programs integrate so deeply into the operating system that it takes a skilled technician several hours to fully diagnose and remove the malicious program. In some extreme cases, we have had no alternative, but to wipe the hard disk clean by deleting all of the files on it and re-installing the operating system.

Obviously this is NOT an ideal situation and we do everything within our power to avoid it. Unfortunately there are some malicious programs that are so intelligent that there is simply no other way of removing them.

Of course you can use Spybot or Ad-Aware as a first attempt at cleaning your machine; however, if you continue to notice that your computer runs slow, if you continue to get crippling pop-ups, or any other of the tell-tale signs discussed earlier, you will need to seek the help of an experienced computer technician.

#2: It is my computer's fault that I continue to get attacked by spyware, malware, and viruses.

In all cases, malware, spyware, and viruses are a result of some action taken by the user (you or an employee). Remember, cyber criminals are *incredibly clever* and gain access to your computer via some of the most innocent and common activities you are performing; that is why it SEEMS as though it is your computer's fault.

For example, one of your employees could innocently download an emoticon software program. Emoticons are the smiley faces and action characters that you see at the bottom of many people's e-mails. In doing so they also (unknowingly) downloaded a payload of spyware and malware to your network.

Other deadly programs to avoid are free "enhanced" web browsers, screen savers, and just about any "cute" programs you come across that are free to download. Always read the terms and conditions before downloading ANY program to look for clauses that allow them (the software vendor) to install spyware programs on your computer. Employees should be restricted from downloading any of these programs from the web and educated to the dangers of these programs.

Having an Internet Usage or Acceptable Use Policy is not enough to protect your company's network. Like many other facets of the business, you must have an easy automated way to enforce the policy and protect your company's valuable data and systems. We all know that a system or policy without accountability just doesn't work for employees.

Installing programs is not the only way a hacker or malware program can access your computer. If you do not have the most up-to-date security patches and virus definitions installed on your computer, hackers can access your PC through a banner ad on the web that you accidentally clicked on or through an e-mail attachment that you opened.

Just recently, hackers have even been able to figure out ways to install malicious programs on your computer via your Internet Explorer web browser EVEN IF YOU DIDN'T CLICK ON ANYTHING OR DOWNLOAD A PROGRAM. Microsoft is constantly providing patches to their operating system software and all it takes is one missed update to leave you completely vulnerable.

Finally, you should COMPLETELY AVOID any and all peer to peer file sharing networks such as KaZaa. These sites are the absolute WORST online activities you can participate in for your computer's health because they are pure breeding grounds for hackers, spyware, malware, and other malicious attacks. Again, most of the infections we see come from employees accessing these websites for personal use on company machines.

#3: If my computer network is working fine right now, I don't need to perform maintenance on it.

This is probably one of the biggest and most deadly misconceptions that most business owners fall victim to. Computer networks are just like cars. If you don't change the oil, change the filter, rotate the tires, flush the transmission, and perform other regular maintenance on your car, it will eventually break down and cost you FAR MORE to repair than the cost of the basic maintenance.

There are certain maintenance checks that need to be done daily (like virus updates and spam filtering), weekly (like system backups and a spyware sweep), and monthly or quarterly like checking for and installing security patches and updates, disk defrag, spyware detection and removal, checking the surge suppressor and the integrity of the hard drive, and so on.

Your computer repair technician should be adamant that you have regular maintenance done on your computer and should offer to set up automatic virus definition updates, spam filtering (to avoid viruses), and automatic system backups that are stored on an OFF SITE location (this protects the backup from fire, flood, or other natural disasters).

If your technician does not press you to let him do this for you, then RUN – don't walk – out of their office. Lack of system maintenance is the NUMBER ONE reason most people end up losing valuable files and incurring heavy computer repair bills. If your technician isn't offering you these services, you need to find someone else to support your computer or network for two reasons:

1. Either they don't know enough to make this recommendation, which is a sure sign they are horribly inexperienced, *OR*
2. They recognize that they are *profiting* from your computer problems and don't want to recommend steps towards preventing you from needing their help on an ongoing basis.

Either reason is a good one to get as far away from that person as possible!

#4: The firewall and security tools provided in the Microsoft Operating System are all the maintenance and protection I need.

Again, this is a terrible misconception. Microsoft does NOT include ALL of the security features to protect your data from viruses, hackers, and data loss or prevent your PC from running slowly. As a matter of fact, there is no one single vendor that provides ALL of the system security features you need to keep your computer and files safe from harm.

Security and protection from these malicious attacks and inappropriate employee online activities takes a multi-faceted, layered approach. Let me outline exactly what you need to make sure your computer network is completely protected.

7 Simple Steps To Secure Your Network From Malicious Attacks and Inappropriate Employee Online Activities To Avoid Expensive Repair Bills

While it's impossible to plan for every potential computer problem or emergency, a little proactive monitoring and maintenance of your network will help you avoid or greatly reduce the impact of the vast majority of computer disasters you could experience.

Unfortunately, I have found that most small business owners are NOT conducting any type of proactive monitoring or maintenance on their network, which leaves them completely vulnerable to the types of disasters you just read about. This is primarily for four reasons:

- #1. They don't understand the importance of regular maintenance.
- #2. Even if they DID understand its importance, they simply do not know what maintenance is required or how to do it.
- #3. They are already swamped with more immediate day-to-day fires demanding their attention. If their network is working fine today, it goes to the bottom of the pile of things to worry about. That means no one is watching to make sure the backups are working properly, the virus protection is up-to-date, that critical security patches are being applied, or that the network is "healthy" overall. (or that employees are not abusing their internet and email resources)
- #4. They assume that their IT guy or provider is handling these things. The problem here is how do you evaluate whether or not these things are being done if you yourself don't know what to check – after all, you have a business to run. The Key to really knowing is: have a built-in accountability system for your provider. If he or she cannot show you detailed daily reports on what he or she is doing to secure and manage threats on your network, then you need to find someone else to support your network for two reasons:
 1. either they don't know enough to check these things, which is a sure sign that they are horribly inexperienced , OR

2. They recognize that they don't know what all to do and as long as they solve your specific problems that you report, they know **you will assume that they have all the other security checkpoints handled.**

Either reason is a good one to consider having a second opinion!

While there are over 45 critical checks and maintenance tasks that need to be performed on a daily, weekly, and monthly basis, I'm going to share with you the 7 that are most important for protecting your company.

Step#1: Make Sure You Are Backing Up Your Files Every Day

It just amazes me how many businesses never back up their computer network. Imagine this: you write the most important piece of information you could ever write on a chalkboard and I come along and erase it. How are you going to get it back? You're not. Unless you can remember it, or if YOU MADE A COPY OF IT, you can't recover the data. It's gone. That is why it is so important to back up your network. There are a number of things that could cause you to lose data files. If the information on the disk is important to you, make sure you have more than one copy of it.

Step #2: Check Your Backups On A Regular Basis To Make Sure They Are Working Properly

This is another big mistake I see. Many business owners set up some type of backup system, but then never check to make sure it's working properly. Worse is that they assume that the IT guy or provider is doing that check on a regular basis.

It's not uncommon for a system to APPEAR to be backing up when in reality, it's not. There are dozens of things that can go wrong and cause your backup to become corrupt and useless. That is why it's not enough to simply back up your system; you have to check it on a regular basis to make sure the data is recoverable in the event of an emergency. Data backups without being able to recover quickly are useless. Data backups are only half of the equation. Returning to business requires that the backup data be quickly and effectively restored for use. The biggest mistake we see when we start serving a new client is: the IT guy or Provider has NEVER tested the backups to ensure they actually work. The worst time to make this discovery is when you need them the most! For a quick litmus test, ask your IT guy NOW when was the last time he/she tested a backup and if the answer is NEVER. Do one today.

Step #3: Keep An Offsite Copy Of Your Backups

What happens if a fire or flood destroys your server AND the backup tapes or drive? This is how hurricane Katrina devastated many businesses that have now been forced into bankruptcy. What happens if your office gets robbed and they take EVERYTHING? Having an offsite backup is simply a smart way to make sure you can get your business back up and running in a relatively short period of time. Again, make sure that your IT Guy is regularly testing the backups and that you are verifying the data is good.

Step #4: Make Sure Your Virus Protection Is ALWAYS On AND Up-To-Date AND Ensure You Have A Multilayered Approach To Network Security

You would have to be living under a rock to not know how devastating a virus can be to your network. With virus attacks coming from spam, downloaded data and music files, instant messages, web sites, and e-mails from friends and clients, you cannot afford to be without up-to-date virus protection.

Not only can a virus corrupt your files and bring down your network, but it can also hurt your reputation. If you or one of your employees unknowingly spreads a virus to a customer, or if the virus hijacks your e-mail address book, you're going to make a lot of people very angry.

Viruses and the hackers that create them have become more sophisticated over the last few years. Unfortunately there is no one silver bullet antivirus program that catches all viruses. To combat this new complexity in virus attacks, we've found that having a multilayered approach is key to stopping viruses. A multi-layered approach involves having two or more antivirus programs on the network and having an at-the edge solution so that viruses are stopped before they even enter the network. It's similar to having a gated community for your neighborhood. Having a gate at the entrance to the neighborhood deters some criminals and makes it more trouble to enter.

Step #5: Set Up A Firewall

Small business owners tend to think that because they are "just a small business", no one would waste time trying to hack in to their network, when nothing could be further from the truth. I've conducted experiments where I connected a single computer to the Internet with no firewall. Within hours, over 13 gigabytes of space was taken over by malicious code and files that I could not delete. The simple fact is that there are thousands of unscrupulous individuals out there who think it's fun to disable your computer just because they can.

These individuals strike randomly by searching the Internet for open, unprotected ports. As soon as they find one, they will delete files or download huge files that cannot be deleted, shutting down your hard drive. They can also use your computer as a zombie for storing pirated software or sending spam, which will cause your ISP to shut YOU down and prevent you from accessing the Internet or sending and receiving e-mail.

If the malicious programs can't be deleted, you'll have to re-format the entire hard drive causing you to lose every piece of information you've ever owned UNLESS you were backing up your files properly (see 1 to 3 above).

Step #6: Update Your System With Critical Security Patches As They Become Available

If you do not have the most up-to-date security patches and virus definitions installed on your network, hackers can access your computer through a simple banner ad or through an email attachment.

Not too long ago Microsoft released a security bulletin about three newly discovered vulnerabilities that could allow an attacker to gain control of your computer by tricking users into downloading and opening a maliciously crafted picture. At the same time, Microsoft released a Windows update to correct the vulnerabilities; but if you didn't have a process to ensure you were applying critical updates as soon as they become available, you were completely vulnerable to this attack.

Here's another compelling reason to ensure your network stays up-to-date with the latest security patches...

Most hackers do not discover these security loopholes on their own. Instead, they learn about them when Microsoft (or any other software vendor for that matter) announces the vulnerability and issues an update. That is their cue to spring into action and they immediately go to work to analyze the update and craft an exploit (like a virus) that allows them access to any computer or network that has not yet installed the security patch.

In essence, the time between the release of the update and the release of the exploit that targets the underlying vulnerability is getting shorter every day.

When the "nimda" worm was first discovered back in the fall of 2001, Microsoft had already released the patch that protected against that vulnerability *almost a year before* (331 days). So network administrators had plenty of time to apply the update. Of course, many still hadn't done so, and the "nimda" worm caused lots of damage. But in the summer of 2003 there were *only 25 days* between the release of the Microsoft update that would have protected against the "blaster" worm and the detection of the worm itself!

Clearly, *someone* needs to be paying close attention to your systems to ensure that critical updates are applied as soon as possible. That is why we highly recommend small business owners without a full-time IT staff allow their consultant to monitor and maintain their network.

Step #7: Make Sure Your Company's Firewall Is Automatically Managed and Secured

You're thinking but I already have a firewall. The truth is standard firewalls just are not secure enough anymore and they are not all created equal. Viruses, Hackers and malicious code are more sophisticated than ever before. The firewall and attempts to break-in need to be monitored constantly so that suspicious activities can be halted before the criminals even enter the company network. Often the hacker will try several attempts to break-in before being successful. The key

to stopping their break-in is to KNOW when they are trying so activities can be halted before they succeed.

It is also a known fact that most data breaches originate on the inside. In the past few months, several clients have contacted us to track activities on employees and unbelievably we helped them verify that their own trusted employees were sending confidential data to their personal email accounts. That is why it is so critical to monitor or stop these attacks as soon as they start. To stop security invasions, you need to immediately respond if they begin suspicious activities.

Unfortunately, I have found that most small business owners are NOT conducting any type of proactive monitoring or maintenance of their companies network activities, which leaves them completely vulnerable to inappropriate employee online activities such as playing online games, online shopping, viewing and downloading porn and inadvertently clicking on damaging emails that are laden with viruses and spyware. This is primarily for five overlooked gaps that most business owners fail to realize about network security:

- #1. They don't understand the importance of stopping such activities as soon as they occur.
- #2. Even if they did get alerted to an attack, they simply do not know what to do with this information.
- #3. They assume their IT guy or the firewall automatically does these activities.

While there are over 10 critical checks and maintenance items that need to be checked every day on a company's network security, I am going to share with you the 5 critical requirements for an effective network security management system.

#1 NETWORK SECURITY REQUIREMENT: Make Sure You Have A Network Security System To Automatically Block Unwanted Employee Online Activities

The problem is most business owners think that having antivirus and a firewall is enough to prevent employees from wasting time and resources by surfing the internet. A small percentage of them have implemented a written internet usage policy or acceptable use policy. As a business owner, we know that written policies are ineffective unless you have a built-in automatic way to enforce it. That is why so many companies have time clocks. The principal is the same here. Unless you have a way to automatically enforce your internet usage policy, its useless.

Therefore, you must have an automatic system that can block crippling employee activities such as:

- ✓ Checking personal email accounts
- ✓ Preventing access to facebook, instant messenger and AOL
- ✓ Stop internet radio and internet shopping access.

#2 NETWORK SECURITY REQUIREMENT: Make Sure You Are Blocking Spam BEFORE It Enters The Network

Most business owners think a spam filter is enough. The problem though is that if the spam enters the network, it slows resources and the email server. The key to eliminating spam is to stop it from even penetrating the email server. This process is accomplished by installing an At-Edge spam filter. These devices stop spam from even entering the network but simultaneously allow the users to check their spam filter and set their own preferences for what is allowed based on what the business owner decides is permissible.

#3 NETWORK SECURITY REQUIREMENT: Provide Safe & Secure Remote Access For All Employees

Most business owners provide access to their network to remote employees or key personnel through Microsoft's remote desktop or terminal services. The problem is that anyone that has a username and password can access the network and all the resources of it this way. To prevent this security hole, you need to install a SECURED remote connection to your network.

Why is this so important? Because employees share information even though they are not supposed to. Employees often share usernames and passwords and this represents a huge risk to a business owner.

Let me explain...

When you terminate an employee, you inactivate their username and password. The problem occurs in that they likely know the usernames and passwords for other employees. The way to absolutely lock-out ex-employees out is to install an open VPN connection. This way –even though the ex-employee may know the username and password – they are not allowed to connect because they no longer have the open vpn SECURED access connection.

#4 NETWORK SECURITY REQUIREMENT: Make Sure Your Network Has the Ability to Fail-Over To An Alternate Internet Connection AUTOMATICALLY

Despite the best practices, firewall, antivirus software etc, your network can still become infected with viruses, spam and spyware. One effective measure to stop it immediately is to tier your internet availability so that if a virus comes in and starts flooding your internet connection, you can have the system automatically stop allowing traffic and transmissions from the infected computer. This automatic process coupled with a system alert enables your IT team to automatically diagnose and stop the troublesome activity. Meanwhile – the rest of the staff is converted over to the alternate or backup internet line and can continue working, sending email and using the Internet. So many times we see a computer on the network get infected with a virus and then the whole network is shutdown because of the one infection. To stop this from happening, it's critical to have a Fail-Over Internet Connection that changes over automatically

when a problem occurs. After all, who can afford to have all of their employees unable to work simultaneously?

#5 NETWORK SECURITY REQUIREMENT: Make Sure You Have Access To Easy-To-Use Management Tools to Control Network and Internet Access Of Your Employees

If you suspect an employee is not performing as they should, you should have tools in place to review how they are spending their time online. With readily available reports, you can evaluate employee performance without them even knowing it. Then corrective action can be taken according to your internet usage policy and procedures.

Want To Be Absolutely Certain That Your Computer Network Is Safe From Spyware, Malware, and Other Threats Including Inappropriate Employee Online Activities?

FREE Problem Prevention Audit for All New Customers

As a prospective customer, we would like to offer you a \$597 Problem Prevention Audit of your company's network for FREE.

During this audit we will do a comprehensive 45-point audit of your computer network to look for potential problems, security loopholes, spyware, and other computer problems that will cause your computers and network to run slow, act funny, crash, and lose data.

We will:

- ✓ Diagnose any computer problems you are experiencing
- ✓ Check your network's security against hacker attacks and viruses
- ✓ Review your network and data backup processes to ensure they are working properly
- ✓ Check that your computer and network equipment does not have any service failures or critical alerts
- ✓ Provide system utilization reports to pinpoint current and potential service interruptions including a list by employee and by system to help you identify installed viruses, malware and spyware
- ✓ Provide written documentation of all critical systems for asset tracking and disaster preparedness purposes

All you have to do is contact us for ANY computer repair or service and we'll do this comprehensive audit for FREE!

**How To Request Your FREE Problem Prevention Audit:
To schedule your 45-Point Problem Prevention Audit and to get more
information about our FIXED FEE service plans:**

- 1. Call me direct at 678-730-2703.**
- 2. Email me at Jennifer@mis-solutions.com.**
- 3. Fax the enclosed form to me at 770-932-4287.**

**“Yes! I Want To Make Sure My Network And
Company’s Data Is Safe From Harm”**

Please sign me up for a FREE 45-Point Problem Prevention Audit so I can make sure I am doing everything possible to secure my network. I understand that I am under **no obligation** to do or to buy anything by requesting this audit.

Please Complete And Fax Back to 770-932-4287

Name: _____

Title: _____

Company: _____

Address: _____

City: _____ ST: _____ Zip: _____

Phone: _____ Fax: _____

E-mail: _____

Number of PCs: _____

Operating System: _____

The MIS Solutions Customer Bill Of Rights

Here is what I promise to deliver if you choose MIS Solutions to service your computers or company network:

1. When you call us with a computer problem, we guarantee that your phone call will be either answered immediately or returned within 60 minutes or less by an experienced technician who can help.
2. You should not have to wait around all day for your computer to be repaired. We understand how important your computer is to you; that is why we offer specific appointment times for repair services.
3. You deserve to get answers to your questions in PLAIN ENGLISH. Our technicians will not talk down to you or make you feel stupid because you don't understand their "geek speak".
4. You deserve complete satisfaction with our products and services. We will do whatever it takes to make you happy. No hassles, no problems.
5. You should EXPECT that no damage will be done to your machine or your data. Before we start working on your computer or network, we will evaluate your problem and alert you to any potential risks involved in fulfilling your job. If there are any risks, they will be explained in full, and your authorization and agreement will be obtained before the work commences. You can also choose to have your data backed up before we start any work on your machine.

A large proportion of our business comes from referrals from happy, satisfied customers. We want you to recommend us and we know that you will only do this if you are happy with the services we provide. That is why we work so hard to go above and beyond the call of duty.

Don't Take Our Word For It; Just Listen To What Our Customers Have To Say...

"We have been working with MIS Solutions for the past seven years because they provide quality service. Keeping our network running is a priority for them, and they understand how crucial it is to our business."

- Yunetta Hamby, Office Manager, Burnette Insurance, Inc.

"I sleep easier at night knowing the MIS team is in my corner, supporting my business, and keeping my systems in tip top shape. Thank you MIS!"

- John Bedard, Bedard Law Group, P.C.

"What impresses me most about MIS Solutions is their knowledge, reliability and responsiveness. Our relationship goes back nearly 10 years and throughout that time, they have always been responsive to us, providing the support and expertise we needed. Good business is

founded on strong relationships. Strong relationships are based on trust, reliability and competence. MIS Solutions demonstrates all of these with each interaction.”

- Joe Doherty, President, Benevox

“The most valuable part of the business relationship for me with MIS is that all of the engineers and staff have worked patiently with me to teach me about the technology and systems we use. I regard everyone at MIS Solutions as business partners. We have learned much more about the technology and systems we need and use. The result is that we are making sound and prudent decisions that make us stronger and more efficient as a company.”

- Kathryn Teague, Operations Manager, National Allergy Supply

“We really like the responsiveness of the MIS Team. They respond quickly to our needs. The MIS TRACK portal system gives us instant notifications on the progress of their work for us. We’ve tried other providers and no other firm can match the quality and responsiveness of MIS’s Greenlight Advanced fixed fee program. They get to the root of technical problems and solve them. I love the fact that MIS can handle all of our applications without me personally having to deal with a lot of other vendors.”

-Gayle Holcomb, Office Manager, Paragon Insurance Service Inc.