

PC Security Checklists

Issue	Check if True	Follow-up Tasks (If you did not check the previous box.)
Is an anti-virus program installed on your computer?		and are completing this checklist for a University computer, you should check with your campus IT or desktop support group to determine if your campus uses a standard virus checking software. This software may also be available for home use.
Is the anti-virus program configured to check every file that gets to your computer (e.g., disks, cd-rom, email and the web)?		Configure your computer properly. Viruses can be distributed in a variety of ways so it is critical that all methods are scanned to reduce the risk of infection/corruption of your computer and its files
Do you check files for viruses on demand (e.g., when sending an attachment via email)?		Scan all files for viruses before sending and before opening them. Viruses are being created every minute and in many different mediums so it is critical that you check all incoming and outgoing files/emails. Failing to do so makes it more likely your computer or someone else's will be infected/corrupted by a virus
Do you check for new virus signatures regularly?		New viruses are being created every minute so it is critical that you check for new virus signatures regularly. Failing to do so makes it more likely your computer will be infected/corrupted by a virus.
Do you monitor virus alert web sites regularly?		New viruses are being created every minute so it is important to know when a new virus has been discovered. Being alert will help you be prepared. Failing to do so makes it more likely your computer will be infected/corrupted by a virus
Do you have firewall software installed on your computer?		There are several personal firewalls available. If you are looking for personal firewall software for a University computer, you should

	<p>check with your campus IT or desktop support group to determine if your campus uses standard personal firewall software. This software may also be available for home use.</p> <p>On a computer, the firewall acts much like a guard when it looks at network traffic destined for or received from another computer. The firewall determines if that traffic should continue on to its destination or be stopped. The firewall "guard" is important because it keeps the unwanted out and permits only appropriate traffic to enter and leave the computer</p>
<p>Do you regularly install software patches to reduce system vulnerability</p>	<p>Set up a patching process or work with your desktop support person to ensure patches are installed in a timely manner.</p> <p>Most vendors provide patches that are supposed to fix bugs in their products.</p> <p>Vendors often provide free patches on their web sites. When you purchase programs, it's a good idea to see if and how the vendor supplies patches, and if and how they provide a way to ask questions about their products.</p> <p>Program vendors also provide a recall-like service. You can receive patch notices through email by subscribing to mailing lists operated by the programs' vendors. Through this type of service, you can learn about problems with your computer even before you discover them and, hopefully, before intruders have the chance to exploit them. Consult the</p>

		<p>vendor's web site to see how to get email notices about patches as soon as they're available.</p> <p>Some vendors have gone beyond mailing lists. They provide programs bundled with their systems that automatically contact their web sites looking for patches. These automatic updates tell you when patches are available, download them, and even install them. You can tailor the update features to do only what you want, such as just telling you something new is waiting but doing nothing more.</p>
<p>If you perform software patches, do you record information (e.g. patch descriptions, patch id, patch url, etc.)?</p>		<p>Maintain records of software patches. This will help you ensure that you have installed critical patches, reduced the risk of corruption of your computer, only installed patches once, and making the process more formal will prompt you to routinely check for patches.</p>
<p>Do you backup operating system and application software when it is first purchased and after patches are applied.</p>		<p>The individual responsible for backing up software and files on a computer varies and depends on whether the computer is connected to network or is "stand-alone". There are different methods used to back-up files. For electronic retrieval, the information could be copied onto a disk or copied to the network. Discuss your options and the best method with your systems administrator</p>
<p>Do you backup data after critical or substantial updates?</p>		<p>The individual responsible for backing up software and files on a computer varies and depends on whether the computer is connected to network or is "stand-alone". There are different methods used to back-up files. For electronic retrieval, the information could be</p>

		copied onto a disk or copied to the network. Discuss your options and the best method with your systems administrator
Do you store backups in a separate location away from your computer?		All backups should be stored in a location separate from that of your computer. This is referred to as storing your backups off-site and ensures that a single disaster does not destroy all copies of program and data files
Do you record backup information (e.g. files backed up, date)?		Maintain records of program and data backups. This will help you when you need to retrieve backups to restore after a disaster and will also make your backup process more formal and likely to be routinely followed.
Are your backups being made to the appropriate media?		Regular backups are your final line of defense against attack. Depending on how much data you have, consider getting a CD-ROM burner. For \$1 per disk, you can have archival backups and avoid reusing media. That way you have a copy of every change you've made. Obviously, this doesn't work if you're managing a large site with more than 500MB of data, but if you're managing more than a casual amount of data, it's essential to make sure you can recover it if need be.
Do you use common words in your password?		You need to create a more secure password. When you create a new password, make sure it: <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the better. • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position.

		<ul style="list-style-type: none"> • Has at least four different characters in your password (no repeats). • Looks like a sequence of random letters and numbers <p>Make sure you:</p> <ul style="list-style-type: none"> • Don't use ANY PART of your logon name for your password. • Don't use any actual word or name in ANY language. • Don't use numbers in place of similar letters. • Don't reuse any portion of your old password. • Don't use consecutive letters or numbers like "abcdefg" or "234567" <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
<p>Do you use repeating or sequential characters/digits in your password?</p>		<p>You need to create a more secure password. When you create a new password, make sure it:</p> <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the better. • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position. • Has at least four different characters in your password (no repeats). • Looks like a sequence of random letters and numbers <p>Make sure you:</p> <ul style="list-style-type: none"> • Don't use ANY PART of your logon name for your

		<p>password.</p> <ul style="list-style-type: none"> • Don't use any actual word or name in ANY language. • Don't use numbers in place of similar letters. • Don't reuse any portion of your old password. • Don't use consecutive letters or numbers like "abcdefg" or "234567" <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
<p>Does your password contain numbers and letters?</p>		<p>You need to create a more secure password. When you create a new password, make sure it:</p> <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the better. • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position. • Has at least four different characters in your password (no repeats). • Looks like a sequence of random letters and numbers <p>Make sure you:</p> <ul style="list-style-type: none"> • Don't use ANY PART of your logon name for your password. • Don't use any actual word or name in ANY language. • Don't use numbers in place of similar letters. • Don't reuse any portion of your old password. • Don't use consecutive letters or numbers like

		<p>"abcdefg" or "234567"</p> <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
Does your password include lower and uppercase characters?		<p>You need to create a more secure password. When you create a new password, make sure it:</p> <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the better. • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position. • Has at least four different characters in your password (no repeats). • Looks like a sequence of random letters and numbers <p>Make sure you:</p> <ul style="list-style-type: none"> • Don't use ANY PART of your logon name for your password. • Don't use any actual word or name in ANY language. • Don't use numbers in place of similar letters. • Don't reuse any portion of your old password . • Don't use consecutive letters or numbers like "abcdefg" or "234567" <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
How long is your password?		<p>You need to create a more secure password. When you create a new password, make sure it:</p> <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the

		<p>better.</p> <ul style="list-style-type: none"> • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position. • Has at least four different characters in your password (no repeats). • Looks like a sequence of random letters and numbers <p>Make sure you:</p> <ul style="list-style-type: none"> • Don't use ANY PART of your logon name for your password • Don't use any actual word or name in ANY language • Don't use numbers in place of similar letters • Don't reuse any portion of your old password • Don't use consecutive letters or numbers like "abcdefg" or "234567" <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
<p>Do you change your password regularly?</p>		<p>You need to create a more secure password. When you create a new password, make sure it:</p> <ul style="list-style-type: none"> • Is at least seven characters in length, and the longer the better. • Includes upper and lower case letters, numerals, symbols. • Has at least one symbol character in the second through sixth position . • Has at least four different characters in your password (no repeats).

		<ul style="list-style-type: none"> Looks like a sequence of random letters and numbers. <p>Make sure you:</p> <ul style="list-style-type: none"> Don't use ANY PART of your logon name for your password. Don't use any actual word or name in ANY language. Don't use numbers in place of similar letters. Don't reuse any portion of your old password. Don't use consecutive letters or numbers like "abcdefg" or "234567" <p>Don't use adjacent keys on your keyboard like "qwerty"</p>
Do you use predictable keywords (e.g., months) and the same creation methods when creating your passwords?		You need to create a more secure password
Do you check the strength of your password at sites such as SecurityStats.com (i.e.,)?		<p>Hackers use software tools that rapidly assess thousands of likely passwords, looking for easy marks. Unscrupulous individuals try to crack your password by trying common words, repeating or sequential numbers/characters, personal information (e.g., child's name, favorite sports team, etc.). Help protect your security and University data/systems by using unlikely or strong passwords, managing your password carefully, and monitoring your accounts.</p>
Is your password stored in batch files, automatic login scripts or terminal function keys?		You need to create a more secure password. Storing your confidential password in files, login scripts and function keys is just as bad as writing it down. You are giving someone the ability to easily use your id and password.

		<p>Think of your password as if it were a key to your home and everything you own, including your reputation. Every action that takes place using your id is your responsibility</p>
<p>Is your password written down?</p>		<p>You need to create a more secure password. You'd be surprised at the number of people who write down their confidential password, and tape it to the monitor; tuck it into a desk drawer next to their computer or an address book. Be sure you:</p> <ul style="list-style-type: none"> • Keep it to yourself. • Do not write it down. • Do not share it with anyone. • Do not check the "remember my password" feature, without considering the value of the data the password protects. • Change your password at least every six months. • Think of your password as if it were a key to your home and everything you own, including your reputation. Every action that takes place using your id is your responsibility
<p>Do you know and understand your responsibilities outlined in University data and computing guidelines/standards (Computer Security & Usage, Data Security & Classification, Electronic Communication, WWW, etc.)?</p>		<p>University data and computing Guidelines detail the standards you are required to follow as a University employee or student in order to use University computing resources. University Data and Computing Policies and Guidelines contain compliance statements that specify the University's response to someone not following these Guidelines. Most indicate that computer/data access may be denied or limited (i.e., to allow for</p>

		<p>the performance of required academic or employment related tasks), and that the violator may also be subject to reprimand, suspension, dismissal, or other disciplinary action.</p> <p>Employees/students may be subject to discipline under these and other University policies</p>
Do you know and understand your responsibilities outlined in state and federal laws (e.g. copyright, computer security, etc.)?		State and Federal laws detail responsibilities and penalties for not adhering to laws related to various data and computing issues.
Is your computer housed in an area or otherwise secured so that it is safeguarded from theft or vandalism (e.g. locked office, cable lockdown system, etc.)?		You should make sure that your system is secured if it is not in a protected area. Remember, if your system is stolen not only do you lose the value of the computer but also the more critical issue is the data that is housed in the system that is lost or compromised (e.g., confidential information made public)
Have the individuals authorized to use the pc been identified?		You and your supervisor, if you are a University employee, need to determine who is authorized to use the pc. Access to the pc means access to the hard drive and the data stored on it. Such access may not be appropriate for every individual
Do you have an inventory of your hardware components (description, serial number, University tag number)?		<p>Make sure your University equipment information is included in University equipment inventory records. This will help with determining asset values and will aid in the reporting of any stolen equipment.</p> <p>Students should also maintain a record of their equipment to aid in the reporting of any stolen equipment.</p>