



# **Cyber Security Seminar**

June 26, 2014

# Table of Contents

Introduction	1
Evaluation	2
Procedures	6
Policies	15
Glossary	21

# Introduction

You've seen the effects of viruses, spam, and spyware on computers — infecting files, blocking up email, and, in some cases, even killing off what might otherwise have been perfectly workable machines. But what's the impact of all this on a business? You have basic IT security measures in place, but are they enough? And if there's something sinister going on in your networks, are you able to detect it? Did you know that 80 percent of businesses without a data protection and recovery plan will go out of business within 18 to 24 months of a disaster or breach?

Understanding the threats your business faces, their potential impact, and the regulations you need to follow is mandatory today. Going the extra step and writing up a security policy — and maybe even acceptable use policies for staff use of company email and Internet — is about protecting yourself even more.

# Evaluation

100 College Boulevard

1. Who will be responsible for ensuring systems are kept up to date and patches are applied to guard against attacks? Who looks after licensing of the software you use?
2. Identify assets and risk factors. Know what technology you have and the risks that threatens them in order to come up with a way to protect your assets.
3. Conduct an impact analysis. Identify potential threats to your business and determine the potential harm. Also, include a recovery process.
4. ***How do you ensure staff members follow your policies on, for example, surfing the Internet — do you rely on them to be honest and follow the rules? Or do you put in place suitable filtering technologies? Security Policy, Acceptable use Policy, Internet and Email policy. Educate your employees why policies are in place and computer self-defense.***
5. Do you have a process for making sure changes to IT hardware and software don't downgrade the security policies already in place?
6. What's your policy on employees using their own IT equipment for business purposes, referred to as bring your own device or BYOD? Including personal storage devices, flash drives and cloud?
7. ***How do you manage the backup of data? Make sure that you have separation of duties, so all the responsibility doesn't fall on one person and you're still secure if they are off sick or on vacation.***
8. ***Do you have a disaster recovery plan? What measures do you have in place to recover from a serious incident such as a fire, network outage, or data breach?***

Businesses also need to be careful regarding the examination of its employees' email messages. Several court opinions have come down on either side of this issue. Businesses that have clear policies stating that any email sent or received on company owned computers is company property have a better leg to stand on here. Generally speaking, organizations should put measures in place to protect all internal information from unwanted disclosure or compromise.

A *security policy* is a statement of intent for how you plan to protect your digital assets and police your organization. It acts as a central repository of guidance for management, staff, and third parties and includes everything from processes and procedures, through people's roles and responsibilities to a description of the technical measures you have in place and how you will recover in the event of an incident.

An *acceptable-use policy* spells out what is and isn't allowed on company time and on company computers and explains the repercussions for disregarding the policy. Without clear guidelines, employees may be exposing the company to malware, sharing confidential information over the Internet, or taking sensitive information offsite on laptops or USB sticks. And they also may be wasting company time!

# BYOD 101

## The risks and rewards of the 'bring your own device' trend in the workplace

Is it time for your business to go BYOD?

Tablets, smartphones, and laptops have changed the way people work. No longer are workers chained to a single desktop computer. And no longer do they store all their important documents, PowerPoint presentations, videos, and reports on one machine.

This has led to a rise in the BYOD (“bring your own device”) movement, with flocks of employees toting their mobile computing devices to work in their backpacks each day. As the Everon business blog notes, this trend isn’t slowing any time soon. The trend is also, more importantly, changing the way businesses across the country operate.

### The risks

Businesses in the past often frowned upon letting employees use their own laptops, smartphones, or tablets at work. The fear? That employees would take important company data out the door with them should they move on to new employment. Other companies worried that employees would infect their computer systems with viruses by connecting their mobile devices to company servers. And a perennial fear is that important customer data might be pried loose from a stolen employee laptop—causing a PR nightmare.

These fears, of course, are still very real ones. However, innovative companies are also realizing that there are several benefits to those businesses who embrace the BYOD movement. The BYOD movement might even give businesses who allow employees to bring their personal devices to work a significant productivity boost.

### The numbers

According to a recent story by PayScale.com, 16 percent of companies surveyed by SAP and NetBase said that a BYOD policy might help boost sales at their companies. The reason? Employees who can use their personal devices at work might also complete more company work after hours. By relying on devices that they are familiar with, they might be able to turn in even more impressive marketing materials and reports. Both of these factors could result in a boost in sales and a boost in company profits.

PayScale cites the experience of security firm ADT, which reported that its sales doubled in some areas when the company let its employees use iPads. Such a move also helps companies cut costs, the PayScale story said, and helps ensure that the move to mobile solutions occurs more efficiently.

Of course, not everyone is a fan of BYOD. The PayScale story found that one in eight companies worry about liability issues should something go wrong with employees using their own devices. A total of 15 percent of respondents said they worried about confidential company information falling into the wrong hands should employees lose mobile devices.

## **Policies**

Trade publication IT Manager Daily recently ran a story on its website providing valuable advice for companies moving toward a BYOD policy.

One of the keys, according to the story, is that companies should create a clear, written BYOD policy that outlines the responsibilities of employees.

For example, the policy could state that employees who share company knowledge stored on their personal devices with outside parties could face disciplinary actions, including losing their jobs.

The written policy should also spell out the responsibility of the company itself. And employees should sign an agreement acknowledging that they have read and understand the company's BYOD policy, according to the IT Manager Daily story.

The Everon blog adds a few other factors that employers need to consider when creating a BYOD policy. First, employers have to determine who pays for mobile voice and data charges. Next, they need to establish minimum system requirements for the mobile devices that their employees want to use.

There are financial factors to consider, too. Employers, for instance, might decide to provide a financial stipend to help employees obtain their mobile devices. And who pays for repairs should a device malfunction? Companies must also determine whether all data stored on employees' mobile devices must also live on the company's file server.

These are important questions, and some of them are challenging. But a written BYOD policy that answers these questions will spare businesses from future problems. Such written policies will also make certain that employees have no excuse for violating companies' BYOD policies.

## **BYOD advantages**

What are the most important advantages associated with a BYOD policy?

The IT Solutions Blog lists many advantages that students receive when they're allowed to bring their own devices to the classroom. Surprisingly, many of these advantages pertain to workers, too.

For instance, IT Solutions Blog says that because students are already familiar and comfortable with their own devices, they can focus on actually learning instead of

deciphering how to use the device. That holds true for employees, too; they won't waste time trying to determine how a particular device works.

At the same time, consumers' personal devices tend to be more up-to-date than much company technology. A BYOD policy can help companies more easily, and inexpensively, keep up with the latest technology.

Another benefit, according to the IT Solutions Blog? Students might be more inspired to continue learning after school if they are allowed to use their own devices at school. That's a benefit that employers should seek, too. Their workers are more likely to work after hours if they can take home company data on their personal devices.

The Everon blog adds a few more benefits of a BYOD policy. The biggest? Employees are more accountable for their own productivity. Workers can't blame malfunctioning company equipment or an inability to access company computers for turning in work or assignments late.

Companies also can save time and costs by not having to create a hardware lifecycle plan or keep inventories of electronic assets. When employees rely on their own devices, such inventories are no longer a necessary job.

Change is always a challenge for companies. And many might still resist putting a BYOD policy in place. Such companies, though, run the risk of being left behind as the computing world turns increasingly to mobile devices.

Yes, a BYOD policy brings risks—real ones. But it also brings real benefits. And a growing number of companies are realizing that these benefits outweigh the risks.

# How can I help protect my computer from viruses?

## Windows 7

---

Protecting your computer from viruses and other threats isn't difficult, but you have to be diligent.

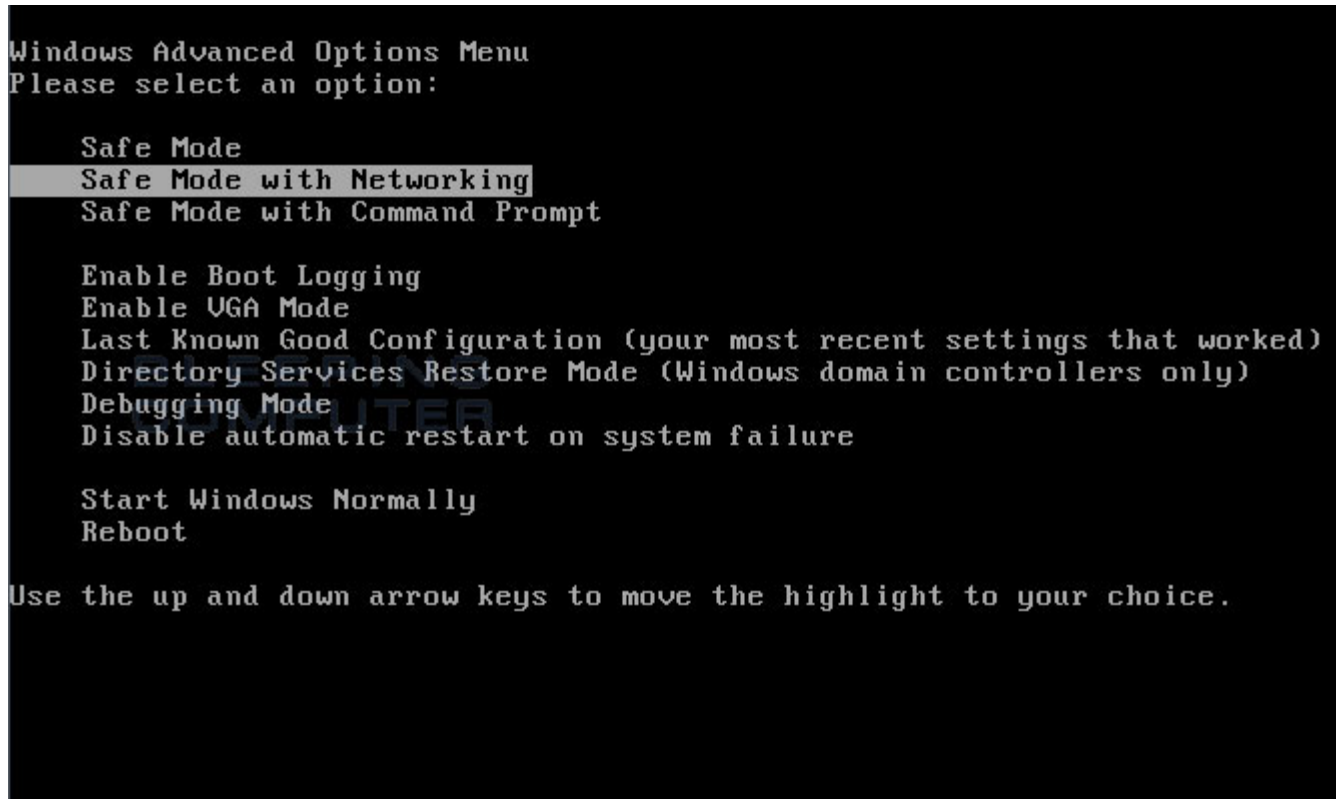
- Install an antivirus program. Installing an antivirus program and keeping it up-to-date can help defend your computer against viruses. Antivirus programs scan for viruses trying to get into your email, operating system, or files. New viruses can appear daily, so check the antivirus manufacturer's website frequently for updates. Some antivirus programs are sold with annual subscriptions that can be renewed as needed, but many are also available for free. Microsoft offers Microsoft Security Essentials, a free antivirus program you can download from the [Microsoft Security Essentials](#) website. You can also visit the [Windows Security software providers](#) webpage to find a third-party antivirus program.
- Don't open email messages from unfamiliar senders, or email attachments that you don't recognize. Many viruses are attached to email messages and will spread as soon as you open the email attachment. It's best not to open any attachment unless it is something you are expecting. Microsoft Outlook and Windows Mail help block potentially dangerous attachments.
- Use a pop-up blocker with your browser. Pop-up windows are small browser windows that appear on top of the website you're viewing. Although most are created by advertisers, they can also contain malicious or unsafe code. A pop-up blocker can prevent some or all of these windows from appearing.  
The Pop-up Blocker feature in Internet Explorer is turned on by default. To learn more about changing its settings or turning it on and off, see [Internet Explorer Pop-up Blocker: frequently asked questions](#).
- Keep Windows updated. Periodically, Microsoft releases special security updates that can help protect your computer. These updates can help prevent viruses and other computer attacks by closing possible security holes. Make sure that Windows receives these updates by turning on Windows automatic updating. To learn how, see [Turn automatic updating on or off](#).
- Use a firewall. Windows Firewall or any other firewall program can help alert you to suspicious activity if a virus or worm attempts to connect to your computer. It can also block viruses, worms, and hackers from attempting to download potentially harmful programs to your computer. To learn more about Windows Firewall, see [Understanding Windows Firewall settings](#).
- Use your browser's privacy settings. Being aware of how websites might use your private information is important to help prevent targeted advertising, fraud, and identity theft. If you're using Internet Explorer, you can adjust your Privacy settings or restore the default settings whenever you want. For details, see [Change Internet Explorer Privacy settings](#).



- Turn on User Account Control (UAC). When changes are going to be made to your computer that require administrator-level permission, UAC notifies you and gives you the opportunity to approve the change. UAC can help keep viruses from making unwanted changes. To learn more about enabling UAC and adjusting the settings, see [Turn User Account Control on or off](#).
- Clear your Internet cache and your browsing history. Most browsers store information about the websites you visit, and information that websites might ask you to provide (such as your name and address). While it can be helpful to have these details stored on your computer, there are times when you might want to delete some or all of them, for example when you're using a public computer and don't want to leave personal information behind. To learn how to clean up your history in Internet Explorer, see [Delete webpage history](#) and [Delete your Internet cookies](#).

# Removal of malware using Malwarebytes

1. Reboot your computer into **Safe Mode with Networking**. To do this, turn your computer off and then back on and immediately when you see anything on the screen, start tapping the **F8** key on your keyboard. Eventually you will be brought to a menu similar to the one below:



Using the arrow keys on your keyboard, select **Safe Mode with Networking** and press **Enter** on your keyboard. If you are having trouble entering safe mode, then please use the following tutorial: [How to start Windows in Safe Mode](#)

Windows will now boot into safe mode with networking and prompt you to login as a user. Please login as the same user you were previously logged in with in the normal Windows mode. Then proceed with the rest of the steps.

2. It is possible that the infection you are trying to remove will not allow you to download files on the infected computer. If this is the case, then you will need to download the files requested in this guide on another computer and then transfer them to the infected computer. You can transfer the files via a CD/DVD, external drive, or USB flash drive.
3. Before we can do anything we must first end the processes that belong to Antivirus Security Pro so that it does not interfere with the cleaning procedure. To do this, please download RKill to your desktop from the following link.

[RKill Download Link](#) - (Download page will open in a new tab or browser window.)

When at the download page, click on the **Download Now** button labeled **iExplore.exe download link**. When you are prompted where to save it, please save it on your **desktop**.

4. Once it is downloaded, double-click on the **iExplore.exe** icon in order to automatically attempt to stop any processes associated with Antivirus Security Pro and other Rogue programs. Please be patient while the program looks for various malware programs and ends them. When it has finished, the black window will automatically close and you can continue with the next step. If you get a message that RKill is an infection, do not be concerned. This message is just a fake warning given by Antivirus Security Pro when it terminates programs that may potentially remove it. If you run into these infections warnings that close RKill, a trick is to leave the warning on the screen and then run RKill again. By not closing the warning, this typically will allow you to bypass the malware trying to protect itself so that RKill can terminate Antivirus Security Pro . So, please try running RKill until the malware is no longer running. You will then be able to proceed with the rest of the guide. **Do not reboot your computer after running RKill as the malware programs will start again.**

**If you continue having problems running RKill, you can download the other renamed versions of RKill from the [RKill download page](#). Both of these files are renamed copies of RKill, which you can try instead. Please note that the download page will open in a new browser window or tab.**

5. Now you should download Malwarebytes Anti-Malware, or MBAM, from the following location and save it to your desktop:

[Malwarebytes Anti-Malware Download Link](#) (Download page will open in a new window)

6. Once downloaded, close all programs and Windows on your computer, including this one.
7. Double-click on the icon on your desktop named **mbam-setup.exe**. This will start the installation of MBAM onto your computer.
8. When the installation begins, keep following the prompts in order to continue with the installation process. Do not make any changes to default settings and when the program has finished installing, make sure you leave both the **Update Malwarebytes Anti-Malware** and **Launch Malwarebytes Anti-Malware** checked. Then click on the **Finish** button. If MalwareBytes' prompts you to reboot, please do not do so.
9. MBAM will now automatically start and you will see a message stating that you should update the program before performing a scan. As MBAM will automatically update itself after the install, you can press the **OK** button to close that box and you will now be at the main program as shown below.



10. On the **Scanner** tab, make sure the **Perform full scan** option is selected and then click on the **Scan** button to start scanning your computer for **Antivirus Security Pro** related files.
11. MBAM will now start scanning your computer for malware. This process can take quite a while, so we suggest you go and do something else and periodically check on the status of the scan. When MBAM is scanning it will look like the image below.



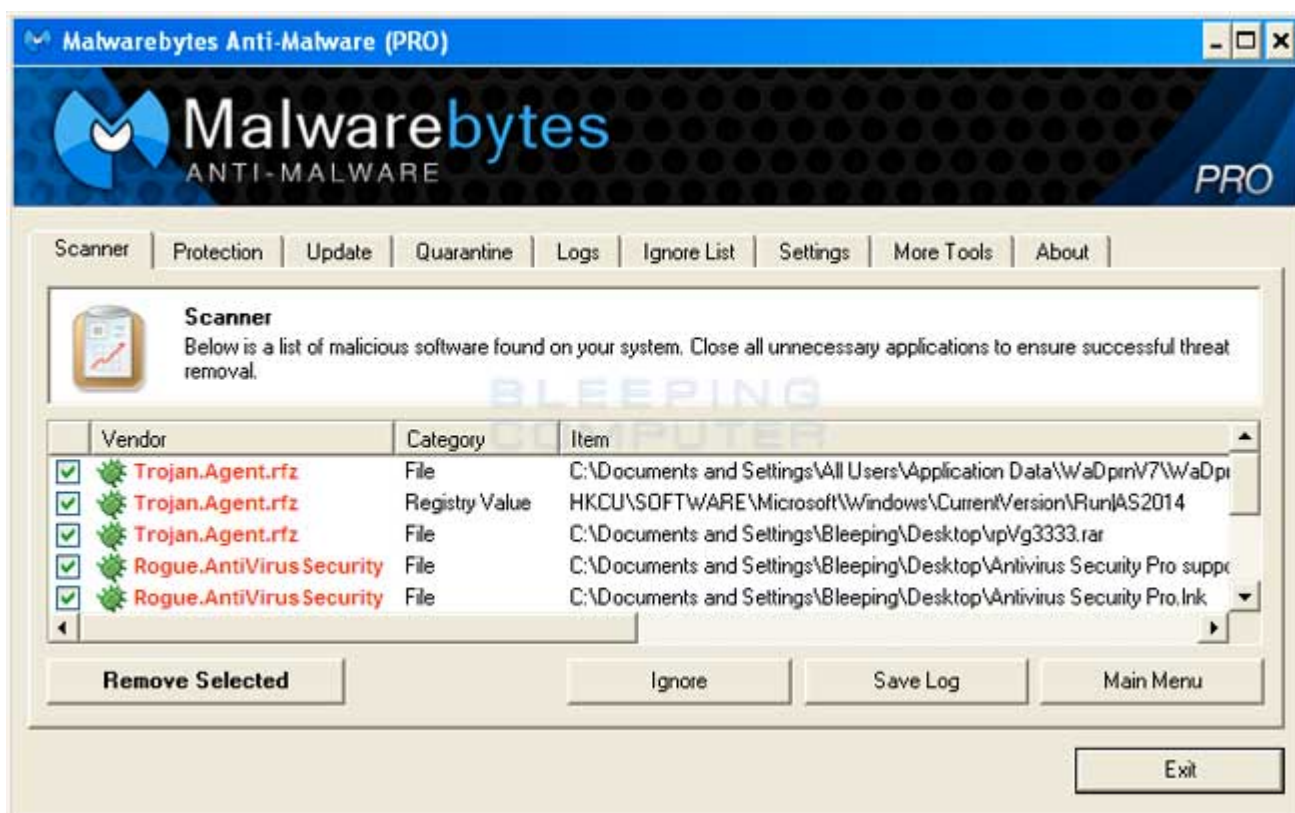
12. When the scan is finished a message box will appear as shown in the image below.



You should click on the OK button to close the message box and continue with the **Antivirus Security Pro** removal process.

13. You will now be back at the main Scanner screen. At this point you should click on the **Show Results** button.

14. A screen displaying all the malware that the program found will be shown as seen in the image below. Please note that the infections found may be different than what is shown in the image.



You should now click on the **Remove Selected** button to remove all the listed malware. MBAM will now delete all of the files and registry keys and add them to the programs quarantine. When removing the files, MBAM may require a reboot in order to remove some of them. If it displays a message stating that it needs to reboot, please allow it to do so. Once your computer has rebooted, and you are logged in, please continue with the rest of the steps.

15. When MBAM has finished removing the malware, it will open the scan log and display it in Notepad. Review the log as desired, and then close the Notepad window.
16. You can now exit the MBAM program.

## Choosing and maintaining good passwords

Because usernames and passwords are the most fundamental level of IT security, it's important that you encourage everyone in the company to choose passwords that are difficult to crack. The following list shows characteristics of hard-to-crack passwords:

- ✓ A combination of upper and lower case letters and numbers
- ✓ Fourteen characters or longer
- ✓ Not composed of words or numbers that other people could guess easily, such as a spouse's or child's name
- ✓ Never use a word found in the dictionary
- ✓ Don't make a pattern on your keyboard

You also need to make sure that everyone takes care of their passwords.

- ✓ Don't write down passwords or leave prompts near the machine used for access.
- ✓ Never leave factory default settings on — using the word "password" or "welcome" as a password is too easy to crack.
- ✓ Never give your password to a third party — even someone from your company, and if you do, change it as soon as you can.

# 7 Smart Things About Passwords

1. The average password is ... pretty terrible. "The overwhelming majority of users choose passwords that contain lower case letters only (i.e. no uppercase, digits, or special characters) unless forced to do otherwise," say Microsoft researchers. What's worse, there's a high statistical likelihood that a password is either 'password' or '123456' or 'qwerty'.
2. Security experts generally agree that a strong password must have four components: length (longer = stronger), a variety of character types and cases, randomness, and uniqueness. "Every password you use can be thought of as a needle hiding in a haystack," says data security expert Steve Gibson. "After all searches of common passwords and dictionaries have failed, an attacker must resort to a 'brute force' search— ultimately trying every possible combination of letters, numbers and then symbols until the combination you chose, is discovered."
3. According to research from Microsoft, the average computer user has 6.5 passwords, each of which is shared across 3.9 different sites. Each user has about 25 accounts that require passwords, and types an average of eight passwords per day.
4. The average password has a bit strength of 40.54. A password with 40 bits of strength would require 240 attempts to exhaust all possibilities during a brute force search. However, a hacker using a brute force search will typically have to try half the possible passwords before finding the correct one. (Password-detection programs can run several billion password guesses per second.) Adding one bit of entropy (i.e. one character) to a password doubles the number of guesses required, which is why longer passwords are far more secure. The National Institute for Standards and Technology recommends a password strength of 80 bits.
5. You don't need a strong password for every site. Just for the important ones. Slate.com tech writer Farhad Manjoo says four or five passwords will suffice, as long as your strong and unique ones are used for the important accounts. "It's perfectly OK to repeat passwords on sites that don't need to be kept very secure," says Manjoo.
6. Manjoo has a helpful shortcut for creating passwords that are both strong and easy to remember. "Start with an original but memorable phrase ... and turn [it] into an acronym. Be sure to use some numbers and symbols and capital letters, too. I like to eat bagels at the airport becomes llteb@ta, and My first Cadillac was a real lemon so I bought a Toyota is M1stCwarlsIbaT."
7. Owners of web-based services and apps have—and should be pressured to use—additional tools to ensure the security of user data. As far as preventing brute force attacks, a simple and effective solution is to have an auto-lockdown system in place when the wrong password is entered multiple times in a row



# Example Acceptable Use Policy for IT Systems

## Using this policy

One of the challenges facing organizations today is enabling employees to work productively while also ensuring the security of the IT network and, crucially, the data on it. Given that technology is continually changing, employees play a significant role in IT security. This policy provides a framework for users to follow when accessing IT systems and the data on them. It is intended to act as a guideline for organizations looking to implement or update their own Acceptable Use Policy.

Feel free to adapt this policy to suit your organization. Where required, adjust, remove or add information according to your needs and your attitude to risk. This is not a comprehensive policy but rather a pragmatic template intended to serve as the basis for your own policy.

Your use of this policy is entirely at your own risk and Sophos therefore makes no conditions, warranties, or representations of any kind, including without limitation fitness for a particular purpose.

This policy should be linked to other policies which support your organization's posture on IT and data security, such as a mobile device security policy, safe password policy and a data security policy.

## Example Policy

### 1. Introduction

This Acceptable Use Policy (AUP) for IT Systems is designed to protect <Company X>, our employees, customers and other partners from harm caused by the misuse of our IT systems and our data. Misuse includes both deliberate and inadvertent actions.

The repercussions of misuse of our systems can be severe. Potential damage includes, but is not limited to, malware infection (e.g. computer viruses), legal and financial penalties for data leakage, and lost productivity resulting from network downtime.

Everyone who works at <Company X> is responsible for the security of our IT systems and the data on them. As such, all employees must ensure they adhere to the guidelines in this policy at all times. Should any employee be unclear on the policy or how it impacts their role they should speak to their manager or IT security officer.

### 2. Definitions

"Users" are everyone who has access to any of <Company X>'s IT systems. This includes permanent employees and also temporary employees, contractors, agencies, consultants, suppliers, customers and business partners.

"Systems" means all IT equipment that connects to the corporate network or access corporate applications. This includes, but is not limited to, desktop computers, laptops, smartphones, tablets, printers, data and voice networks, networked devices, software, electronically-stored data, portable data storage devices, third party networking services, telephone handsets, video conferencing systems, and all other similar items commonly understood to be covered by this term.

### **3. Scope**

This is a universal policy that applies to all Users and all Systems. For some Users and/or some Systems a more specific policy exists: in such cases the more specific policy has precedence in areas where they conflict, but otherwise both policies apply on all other points.

This policy covers only internal use of <Company X>'s systems, and does not cover use of our products or services by customers or other third parties.

Some aspects of this policy affect areas governed by local legislation in certain countries (e.g., employee privacy laws): in such cases the need for local legal compliance has clear precedence over this policy within the bounds of that jurisdiction. In such cases local teams should develop and issue users with a clarification of how the policy applies locally.

Staff members at <Company X> who monitor and enforce compliance with this policy are responsible for ensuring that they remain compliant with relevant local legislation at all times.

### **4. Use of IT Systems**

All data stored on <Company X>'s systems is the property of <Company X>. Users should be aware that the company cannot guarantee the confidentiality of information stored on any <Company X> system except where required to do so by local laws.

<Company X>'s systems exist to support and enable the business. A small amount of personal use is, in most cases, allowed. However it must not be in any way detrimental to users own or their colleagues productivity and nor should it result in any direct costs being borne by <Company X> other than for trivial amounts (e.g., an occasional short telephone call).

<Company X> trusts employees to be fair and sensible when judging what constitutes an acceptable level of personal use of the company's IT systems. If employees are uncertain they should consult their manager.

Any information that is particularly sensitive or vulnerable must be encrypted and/or securely stored so that unauthorised access is prevented (or at least made extremely difficult). However this must be done in a way that does not prevent—or risk preventing—legitimate access by all properly-authorized parties.

<Company X> can monitor the use of its IT systems and the data on it at any time. This may include (except where precluded by local privacy laws) examination of the content stored within the email and data files of any user, and examination of the access history of any users.

<Company X> reserves the right to regularly audit networks and systems to ensure compliance with this policy.

### **5. Data Security**

If data on <Company X>'s systems is classified as confidential this should be clearly indicated within the data and/or the user interface of the system used to access it. Users must take all necessary steps to prevent unauthorized access to confidential information.

Users are expected to exercise reasonable personal judgement when deciding which information is confidential.

Users must not send, upload, remove on portable media or otherwise transfer to a non-<Company X> system any information that is designated as confidential, or that they should reasonably regard as being

confidential to <Company X>, except where explicitly authorized to do so in the performance of their regular duties.

Users must keep passwords secure and not allow others to access their accounts. Users must ensure all passwords comply with <Company X>'s safe password policy.

Users who are supplied with computer equipment by <Company X> are responsible for the safety and care of that equipment, and the security of software and data stored it and on other <Company X> systems that they can access remotely using it.

Because information on portable devices, such as laptops, tablets and smartphones, is especially vulnerable, special care should be exercised with these devices: sensitive information should be stored in encrypted folders only. Users will be held responsible for the consequences of theft of or disclosure of information on portable systems entrusted to their care if they have not taken reasonable precautions to secure it.

All workstations (desktops and laptops) should be secured with a lock-on-idle policy active after at most 10 minutes of inactivity. In addition, the screen and keyboard should be manually locked by the responsible user whenever leaving the machine unattended.

Users who have been charged with the management of those systems are responsible for ensuring that they are at all times properly protected against known threats and vulnerabilities as far as is reasonably practicable and compatible with the designated purpose of those systems.

Users must at all times guard against the risk of malware (e.g., viruses, spyware, Trojan horses, rootkits, worms, backdoors) being imported into <Company X>'s systems by whatever means and must report any actual or suspected malware infection immediately.

## **6. Unacceptable Use**

All employees should use their own judgment regarding what is unacceptable use of <Company X>'s systems. The activities below are provided as examples of unacceptable use, however it is not exhaustive. Should an employee need to contravene these guidelines in order to perform their role, they should consult with and obtain approval from their manager before proceeding.

- All illegal activities. These include theft, computer hacking, malware distribution, contravening copyrights and patents, and using illegal or unlicensed software or services. These also include activities that contravene data protection regulations.
- All activities detrimental to the success of <Company X>. These include sharing sensitive information outside the company, such as research and development information and customer lists, as well as defamation of the company.
- All activities for personal benefit only that have a negative impact on the day-to-day functioning of the business. These include activities that slow down the computer network (e.g., streaming video, playing networked video games).
- All activities that are inappropriate for <Company X> to be associated with and/or are detrimental to the company's reputation. This includes pornography, gambling, inciting hate, bullying and harassment.
- Circumventing the IT security systems and protocols which <Company X> has put in place.

## **7. Enforcement**

<Company X> will not tolerate any misuse of its systems and will discipline anyone found to have contravened the policy, including not exercising reasonable judgment regarding acceptable use. While each situation will be judged on a case-by-case basis, employees should be aware that consequences may include the termination of their employment.

Use of any of <Company X>'s resources for any illegal activity will usually be grounds for summary dismissal, and <Company X> will not hesitate to cooperate with any criminal investigation and prosecution that may result from

## Sample E-mail Policy

**Note: This policy is for informational purposes only.** No reliance should be placed on this document without legal counsel. All electronic policies should be developed with the assistance of a corporate attorney and human resources director/manager.

ABC Co. provides employees with electronic communication tools, including an e-mail system. This email policy, which governs employee use of the company's e-mail system, applies to e-mail use at ABC's headquarters and district offices, as well as remote locations, including, but not limited to, employee homes, airports, hotels, and client and supplier offices. The company's e-mail rules and policies apply to full-time employees, part-time employees, independent contractors, interns, consultants, suppliers, clients, and other third parties. Any employee who violates ABC's e-mail rules and policies is subject to disciplinary action, up to and including termination.

### **E-mail Exists for Business Purposes**

ABC allows e-mail access primarily for business purposes. Employees may use the company's e-mail system for personal use only in accordance with this policy. Employees are prohibited from using personal e-mail software (e.g., Yahoo!, Hotmail, or AOL.) for business or personal communications at the office.

### **Authorized Personal E-mail Use**

Employees may use e-mail to communicate with spouses, children, domestic partners, and other family members. Employees' personal use of e-mail is limited to lunch breaks and work breaks only. Employees may not use e-mail for personal purposes during otherwise productive business hours. Employees are prohibited from using e-mail to operate a business, conduct an external job search, solicit money for personal gain, campaign for political causes or candidates, or promote or solicit funds for a religious or other personal cause.

### **Employees Have No Reasonable Expectation of Privacy**

E-mail messages created and transmitted on ABC computers are the property of the company. ABC reserves the right to monitor all e-mail transmitted via the company's computer system. Employees have no reasonable expectation of privacy when it comes to business and personal use of ABC's e-mail system.

### **E-mail Monitoring Activities**

The company reserves the right to monitor, inspect, copy, review, and store any and all employee e-mail use at any time and without prior notice. In addition, ABC may monitor, inspect, copy, review, and store any files, information, software, and other content created, sent, received, downloaded, uploaded, accessed, or stored through the company's e-mail system. ABC reserves the right to disclose e-mail information and images to regulators, courts, law enforcement agencies, and other third parties without the employee's consent.

### **Offensive Content and Harassing or Discriminatory Activities Are Banned**

Employees are prohibited from using e-mail to engage in activities or transmit content that is harassing, discriminatory, menacing, threatening, obscene, defamatory, or in any way objectionable or offensive.

### **Employees Are Prohibited From Using E-mail to:**

1. Send, receive, solicit, print, copy, or reply to text, images, or jokes that disparage others based on their race, religion, color, gender, sex, sexual orientation, national origin, veteran status, disability, ancestry, or age.
2. Send, receive, solicit, print, copy, or reply to messages that are disparaging or defamatory.
3. Spread gossip, rumors, or innuendos about employees, clients, suppliers, or other outside parties.
4. Send, receive, solicit, print, copy, or reply to sexually oriented messages or images.
5. Send, receive, solicit, print, copy, or reply to messages or images that contain foul, obscene, disrespectful, or adult-oriented language.

6. Send, receive, solicit, print, copy, or reply to messages or images that are intended to alarm others, embarrass ABC, negatively impact employee productivity, or harm employee morale.

**Confidential, Proprietary, and Personal Information Must Be Protected**

Unless authorized to do so, employees are prohibited from using e-mail to transmit confidential information to outside parties. Employees may not access, send, receive, solicit, print, copy, or reply to confidential or proprietary information about ABC Co., its employees, clients, suppliers, and other business associates. Confidential information includes, but is not limited to, client lists, credit card numbers, Social Security numbers, employee performance reviews, salary details, trade secrets, passwords, and information that could embarrass ABC and its employees if the information were disclosed to the public.

**Do Not Use E-mail to Communicate With Lawyers**

To preserve all communication privileges between lawyers and clients, never use e-mail to seek legal advice or pose a legal question.

**Business Record Retention**

E-mail messages are written business records and are subject to ABC's rules and policies for retaining and deleting business records. Please refer to the company's business record retention policy for more information.

**Violations**

These guidelines are intended to provide ABC employees with general examples of acceptable and unacceptable uses of the company's e-mail system. A violation of this policy may result in disciplinary action up to and including termination.

**Acknowledgement**

If you have questions about the above policies and procedures, address them to the compliance officer or chief information officer before signing the following agreement.

I have read ABC's e-mail policy and agree to abide by it. I understand that a violation of any of the above policies and procedures may result in disciplinary action, up to and including my termination.

\_\_\_\_\_  
Employee Name (Printed)

\_\_\_\_\_  
Employee Signature

\_\_\_\_\_  
Date

# Glossary

Word/Term	Definition
<b>Access control</b>	Controlling who has access to a computer or online service and the information it stores.
<b>Adware</b>	Software that automatically plays, displays, or downloads advertisements to a computer, often in exchange for the right to use a program without paying for it. The advertisements seen are based on monitoring of browser habits. Most adware is safe to use, but some can serve as spyware, gathering information about you from your hard drive, the websites you visit, or even your keystrokes. Certain types of adware have the capability to capture or transmit personal information.
<b>Antispam</b>	A type of application that defends against the threats that spam poses (such as viruses, phishing attempts, and denial-of-service attacks) and reduces the amount of spam entering an email system.
<b>Antivirus software</b>	A type of software that scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete, or quarantine any files, directories, or disks affected by the virus. The term <i>antimalware</i> is preferred because it covers more threats.
<b>Asset</b>	Something of value to a person, business or organization.
<b>Authentication</b>	The process to verify that someone is who they claim to be when they try to access a computer or online service.
<b>Backdoor</b>	A backup is a duplicate copy of data made for archiving purposes or for protection against damage and loss. A backup is usually kept physically separate from the originals for recovery when originals are damaged or lost.
<b>Backing up</b>	To make a copy of data stored on a computer or server to lessen the potential impact of failure or loss.
<b>Bot</b>	Short for "robot," a computer that has been infected with malicious software without the user's knowledge. Once the computer has been affected, a cybercriminal can send commands to it and other infected machines over the Internet. Since the compromised

	computers blindly follow the commands of the cybercriminals, infected machines are also called zombies.
<b>Botnet (bot network)</b>	Short for "robot network," a botnet is a network of hijacked computers controlled remotely by a hacker. The hacker can use the network to send spam and launch Denial of Service (DoS) attacks, and may rent the network to other cybercriminals. A single computer in a botnet can automatically send thousands of spam messages per day. The most common spam messages come from zombie computers.
<b>Bring your own device (BYOD)</b>	The authorized use of personally owned mobile devices such as smartphones or tablets in the workplace.
<b>Broadband</b>	High-speed data transmission system where the communications circuit is shared between multiple users.
<b>Browser hijacker</b>	A type of malware that alters your computer's browser settings so that you are redirected to websites that you had no intention of visiting. Most browser hijackers alter browser home pages, search pages, search results, error message pages, or other browser content with unexpected or unwanted content.
<b>Brute-force attack</b>	A hacking method used to find passwords or encryption keys by trying every possible combination of characters until the correct one is found.
<b>Bug</b>	An unintentional fault, error, failure, or mistake in a software program that can produce an incorrect or unexpected result or cause a program to behave in unintended ways.
<b>Business continuity management</b>	Preparing for and maintaining continued business operations following disruption or crisis.
<b>Cache</b>	Pronounced like "cash," a cache stores recently used information in a place where it can be accessed extremely fast. Computers have a disk cache; this stores information that the user has recently read from the hard disk. Web browsers also use a cache to store the pages, images, and URLs of recently visited websites on the user's hard drive. When users visit web pages that they have been to recently, the pages and images don't have to be downloaded again.
<b>Carding</b>	A technique used by thieves to verify the validity of stolen card data. The thief will use the card information on a website that has



	<p>real-time transaction processing. If the transaction is processed successfully then the thief knows the card is still good. The purchase is usually for a small amount to avoid using the card's limit and to avoid attracting the attention of the card owner.</p>
<b>Certification</b>	<p>Declaration that specified requirements have been met.</p>
<b>Certification body</b>	<p>An organization that provides independent standard certification services.</p>
<b>Chargeback</b>	<p>A payment card transaction where the supplier initially receives payment but the transaction is later rejected by the cardholder or the card issuing company. The supplier's account is then debited with the disputed amount.</p>
<b>Cloud computing</b>	<p>Cloud computing refers to applications and services that are offered over the Internet. These services are offered from data centers around the world that collectively are referred to as the "cloud."</p>
<b>Common text</b>	<p>A structure and series of requirements defined by the International Organization for Standardization, that are being incorporated in all management system International Standards as they are revised.</p>
<b>Cookie</b>	<p>Small amounts of data generated by a website and saved by your web browser. Websites use cookies to identify users who revisit their sites, and are most commonly used to store login information for a specific site. When a server receives a browser request that includes a cookie, the server can use the information stored in the cookie to customize the website for the user. Whenever a user checks the box "Remember me on this computer," the website will generate a login cookie once the user successfully logs in. Each time users revisit the site, they may only need to enter their password or may not need to login at all. Cookies can be used to gather more information about a user than would be possible without them.</p>
<b>DAT files</b>	<p>Also known as a data file, these files are used to update software programs, sent to users via the Internet. .DAT files contain up-to-date virus signatures and other information antivirus products use to protect your computer against virus attacks. .DAT files are also known as detection definition files and signatures.</p>

<b>Data</b>	<p>A broad term to describe information that has been translated into a form that is more convenient to move or process.</p> <p>Data can be in the form of text documents, images, audio files, software programs, and many more forms. Data can be processed on a computer or a mobile device, such as a mobile phone or tablet.</p>
<b>Data server</b>	<p>A computer or program that provides other computers with access to shared files over a network.</p>
<b>Declaration of conformity</b>	<p>Confirmation issued by the supplier of a product that specified requirements have been met.</p>
<b>Denial of service (DoS)</b>	<p>An attack specifically designed to prevent a system from functioning properly as well as denying access to the system by authorized users. Hackers can cause denial-of-service attacks by destroying or modifying data or by overloading the system's servers until service to authorized users is delayed or prevented.</p>
<b>Dictionary attack</b>	<p>Method of breaking into a password-protected computer, mobile device, or online account by entering every word in a dictionary as a password.</p>
<b>DMZ</b>	<p>Segment of a network where servers accessed by less trusted users are isolated. The name is derived from the term "demilitarized zone".</p>
<b>Domain name</b>	<p>This is a name that identifies a website; for example, mcafee.com is the domain name of McAfee's website. Each domain name is associated with an IP address. Domain names are used in URLs to identify particular web pages.</p>
<b>Downloading</b>	<p>This is the process in which data is sent to your computer. Whenever you receive information from the Internet, you are downloading it to your computer. For example, you may have to download an update for your web browser. The opposite of this process, is sending information to another computer is called uploading.</p>
<b>Dropper</b>	<p>This is an executable file, created specifically to introduce a virus, worm, or Trojan on a computer system.</p>
<b>Encryption</b>	<p>Encryption is a security method of coding or scrambling data so that it can be decoded or read only by authorized users. This is</p>


	commonly used to secure websites, online purchases, and other transactions.
<b>Ethernet</b>	Communications architecture for wired local area networks based upon <u>IEEE 802.3</u> standards.
<b>Executable file (.exe)</b>	A type of computer file that when opened runs a program or series of instructions contained in the file. These types of files have the potential to be dangerous since they run code when opened, and are often used by cybercriminals to distribute viruses, malware, and spyware.
<b>Exploit</b>	A piece of software that takes advantage of a bug, glitch, or design flaw in software in order to cause unintended or unanticipated behavior on computer software. This can include gaining control of a computer system, changing access privileges, or denying access or resources to users.
<b>False negative</b>	An error that occurs when antivirus software fails to detect that an infected file is truly infected. False negatives are more serious than false positives, although both are undesirable. False negatives are more common with antivirus software because they may miss a new or a heavily modified virus.
<b>False positive</b>	An error that occurs when antivirus software wrongly claims that a virus is infecting a clean file. False positives usually occur when the string chosen for a given virus signature is also present in another program.
<b>Firewall</b>	A piece of hardware or software that is designed to block unauthorized access while permitting authorized communications. It is configured to permit or deny network transmissions based upon a set of rules. They are designed to protect the network's resources from users on other networks.
<b>Gap analysis</b>	The comparison of actual performance against expected or required performance.
<b>Geolocation</b>	Term used to describe the capability to detect and record where you and other people are located. Geolocation information can be obtained in a number of ways, including using data from a user's IP address, MAC address, RFID, Wi-Fi connection location, or GPS coordinates.

<b>Geotagging</b>	Process of adding geographical identification data to various types of media, such as a photograph or video taken with your camera or mobile device. This data usually consists of latitude and longitude coordinates, and they can also contain altitude, bearing, distance, and place names.
<b>Hacker</b>	<p>A broad term for a person who uses programming skills and technical knowledge to create and modify computer software and hardware by finding weaknesses and exploiting them, including computer programming, administration, and security-related items. Hackers can be motivated by a number of reasons both positive and negative, such as profit, protest, or challenge. Criminal hackers create malware in order to commit crimes. See also: malware, cybercriminals, cybergangs.</p> <p>In the early days of computing, hacker was a term used to describe a programmer who had a curiosity and appreciation of programs and systems and how they worked. Over time, however, the term gained a negative connotation and began to refer to someone who uses the knowledge to break into other people's systems to steal information and cause havoc. We also call programmers who use their skills for harm "crackers."</p>
<b>Hard disk</b>	The permanent storage medium within a computer used to store programs and data.
<b>Hole</b>	A vulnerability in the design software and/or hardware that allows the circumvention of security measures.
<b>Host</b>	A term often used to describe the computer file to which a virus attaches itself. Most viruses run when the computer or user tries to use the host file.
<b>Hotspot</b>	A hotspot is a site that offers Internet access over a wireless connection. Hotspots typically use Wi-Fi technology and are generally found in coffee shops and various other public locations.
<b>Hyperlink (link)</b>	A clickable word, phrase, or image on a website that once clicked takes the user from one web page to another, or to another resource on the Internet. They are typically underlined or set apart by a different color. When you move your cursor over a hyperlink, whether text or image, the arrow should change to a small hand pointing at the link.

<b>Identification</b>	The process of recognizing a particular user of a computer or online service.
<b>Infected</b>	This term refers to the condition of a file after a virus, spyware, or malware has inserted malicious code into it. Computer systems are infected if a virus or Trojan is installed and running on that system. Static malware, such as viruses and Trojans with entirely malicious code, is also said to be infected. If a potentially unwanted program is installed on a system, the system is not considered infected, even though there may be other consequences.
<b>Information harvesters</b>	People who supply stolen data but do not necessarily use it to commit fraud. The information obtained by harvesters is sold to criminal networks that trade the information in Internet back alleys.
<b>Infrastructure-as-a-service (IaaS)</b>	Provision of computing infrastructure (such as server or storage capacity) as a remotely provided service accessed online (ie via the internet).
<b>Inspection certificate</b>	A declaration issued by an interested party that specified requirements have been met.
<b>Instant messaging</b>	Chat conversations between two or more people via typing on computers or portable devices.
<b>International Mobile Equipment Identity (IMEI)</b>	A number 15 or 17 digits in length that is unique to each mobile phone and tablet. It is used to identify users on the Global System for Mobile Communications (GSM) and the Universal Mobile Telecommunications System (UMTS). It is usually found printed inside the battery compartment of the phone. If a mobile phone is lost or stolen, the owner can call the network provider and instruct them to blacklist the phone based on the IMEI number and make it useless on the network.
<b>Internet Protocol (IP) address</b>	An IP address is a unique numerical label assigned to a device, such as a computer or other device on a network, including the Internet. IP addresses allow computers, routers, printers, and other devices to identify one another to communicate
<b>Internet service provider (ISP)</b>	Company that provides access to the internet and related services.

<b>Intrusion detection system (IDS)</b>	Program or device used to detect that an attacker is or has attempted unauthorized access to computer resources.
<b>Intrusion prevention system (IPS)</b>	Intrusion detection system that also blocks unauthorized access when detected.
<b>IOS</b>	Apple's brand name for its mobile operating system.
<b>Jailbreaking</b>	Process of removing limitations imposed by Apple on devices running the iOS operating system (iPhone, iPad, and iPod). Users do this to gain root access to the operating system to be able to install apps obtained through means other than the official App Store. While this can allow the user greater control of what is installed on the device, it can also cause data corruption and make the device less secure.
<b>Keyboard logger</b>	Software that tracks or logs the keys struck on a keyboard, typically in a covert manner so that the person using the keyboard is unaware that their actions are being monitored. This is usually done with malicious intent to collect information including instant messages, email text, email addresses, passwords, credit card and account numbers, addresses, and other private data.
<b>Leased circuit</b>	Communications link between two locations used exclusively by one organization. In modern communications, dedicated bandwidth on a shared link reserved for that user.
<b>Local area network (LAN)</b>	Communications network linking multiple computers within a defined location such as an office building.
<b>Macro virus</b>	Malware (ie malicious software) that uses the macro capabilities of common applications such as spreadsheets and word processors to infect data.
<b>Mail bomb</b>	An excessively large email (typically many thousands of messages) or one large message sent to a user's email account. This is done to crash the system and prevent genuine messages from being received.
<b>Malware</b>	A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.

<b>Media access control (MAC) address</b>	A hardware identification number that is a unique code assigned to every piece of hardware that connects to the Internet. This includes Internet-capable phones, network interface cards for desktop and notebook computers, wireless access cards, and even some memory cards. The MAC address is manufactured into every network card, such as an Ethernet card or Wi-Fi card, and can't be changed.
<b>Management system</b>	A set of processes used by an organization to meet policies and objectives for that organization.
<b>Network</b>	A network can consist of two or more computers, mobile devices (phones and tablets), gaming devices, Internet connected TVs, etc. connected to each other. Networks can be connected by cables or wirelessly. The purpose of a network is to share files and information.
<b>Network firewall</b>	Device that controls traffic to and from a network.
<b>Outsourcing</b>	Obtaining services by using someone else's resources.
<b>Passing off</b>	Making false representation that goods or services are those of another business.
<b>Password</b>	A secret series of characters used to authenticate a person's identity.
<b>Password cracker</b>	Software designed to enable a user or administrator to recover lost or forgotten passwords from accounts or data files. In the hands of an attacker, these tools offer access to confidential information and are a security and privacy threat.
<b>Peer-to-peer (P2P) networking</b>	A distributed system of file sharing in which any computer on the network can see any other computer on the network. Users can access each others' hard drives to download files. This type of file sharing is valuable, but it brings up copyright issues for music, movies, and other shared-media files. Users are also vulnerable to viruses, Trojans, and spyware hiding in files.
<b>Personal firewall</b>	Software running on a PC that controls network traffic to and from that computer.
<b>Personal information</b>	Personal data relating to an identifiable living individual.

<b>Pharming</b>	The process of redirecting traffic to a fake website, often through the use of malware or spyware. A hacker sets up a fraudulent website that looks like a legitimate website in order to capture confidential information from users.
<b>Phishing</b>	A form of criminal activity using social engineering techniques through email or instant messaging. Phishers attempt to fraudulently acquire other people's personal information, such as passwords and credit card details, by masquerading as a trustworthy person or business in an apparently official electronic communication. Typically, phishing emails request that recipients click on the link in the email to verify or update contact details or credit card information. Like spam, phishing emails are sent to a large number of email addresses, with the expectation that someone will act on the information in the email and disclose their personal information. Phishing can also happen via text messaging or phone.
<b>Platform-as-a-service (PaaS)</b>	The provision of remote infrastructure allowing the development and deployment of new software applications over the internet.
<b>Portable device</b>	A small, easily transportable computing device such as a smartphone, laptop or tablet computer.
<b>Proxy server</b>	Server that acts as an intermediary between users and others servers, validating user requests.
<b>Quarantine</b>	The isolation of files that are suspected of containing a virus, spam, suspicious content, or PUPs. Quarantined files cannot be opened or executed.
<b>Quick response (QR) code</b>	 <p>A two-dimensional code that can be scanned with a QR barcode reader or a camera-enabled smartphone with QR reader software. Once a QR code is scanned, it can direct a user to just about anything: a web page, call a phone number, or an SMS text message. QR codes provide organizations with a quick and easy way to direct their customers to online content. QR codes are often found in magazines, product packaging, on advertisements, online, and in other marketing collateral.</p>
<b>Ransomware</b>	Malicious software created by a hacker to restrict access to the computer system that it infects and demand a ransom paid to the creator of the malicious software for the restriction to be removed.



	Some forms of ransomware may encrypt files on the system's hard drive, while others may simply lock the system and display messages to coax the user into paying.
<b>Redirect</b>	A method used to direct someone or something to a different place than was intended. Cybercriminals can use these to route a legitimate website's traffic to a counterfeit website.
<b>Remote administration tool (RAT)</b>	Software designed to give an administrator remote control of a system. Hackers can install malicious RAT software on a computer without the user's knowledge and take control of it remotely without the user's knowledge. RATs can be installed by opening an infected attachment, clicking links in a popup window, or through any other software that poses as legitimate.
<b>Replication</b>	The process by which a virus makes copies of itself to carry out subsequent infections. Replication is one of the major criteria separating viruses from other computer programs.
<b>Restore</b>	The recovery of data following computer failure or loss.
<b>Risk</b>	Something that could cause an organization not to meet one of its objectives.
<b>Risk assessment</b>	The process of identifying, analyzing and evaluating risk.
<b>Rootkits</b>	A stealthy type of malware that is designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer. Rootkits are the hardest type of invasive software to detect and nearly impossible to remove. As eluded to in the name, they dig into the root of a hard drive. They are designed to steal passwords and identifying information.
<b>Router</b>	Device that directs messages within or between networks.
<b>Screen scraper</b>	A virus or physical device that logs information sent to a visual display to capture private or personal information.
<b>Security control</b>	Something that modifies or reduces one or more security risks.
<b>Security information and event</b>	Process in which network information is aggregated, sorted and correlated to detect suspicious activities.

<b>management (SIEM)</b>	
<b>Security perimeter</b>	A well-defined boundary within which security controls are enforced.
<b>Server</b>	Computer that provides data or services to other computers over a network.
<b>Smartphone</b>	A mobile phone built on a mobile computing platform that offers more advanced computing ability and connectivity than a standard mobile phone.
<b>Software-as-a-service (SaaS)</b>	The delivery of software applications remotely by a provider over the internet; perhaps through a web interface.
<b>Spam</b>	Unsolicited junk email; can contain malicious code in attachments or links to malicious code stored elsewhere.
<b>Spoofing</b>	Programming computers to impersonate others. IP spoofing uses a fake IP address to access a network.
<b>Spyware</b>	Malware that passes information about a computer user's activities to an external party.
<b>Supply chain</b>	A set of organizations with linked resources and processes involved in the production of a product.
<b>Tablet</b>	An ultra-portable, touch screen computer that shares much of the functionality and operating system of smartphones, but generally has greater computing power.
<b>Threat</b>	Something that could cause harm to a system or organization.
<b>Threat actor</b>	A person who performs a cyber-attack or causes an accident.
<b>Trojan</b>	A type of malware that appears harmless, but has some hidden malicious intent.

<b>Two-factor authentication</b>	Obtaining evidence of identity by two independent means, such as knowing a password and successfully completing a smartcard transaction.
<b>Username</b>	The short name, usually meaningful in some way, associated with a particular computer user.
<b>User account</b>	The record of a user kept by a computer to control their access to files and programs.
<b>Virtual private network (VPN)</b>	Link(s) between computers or local area networks across different locations using a wide area network that cannot access or be accessed by other users of the wide area network.
<b>Virus</b>	Malware that is loaded onto a computer and then run without the user's knowledge or knowledge of its full effects.
<b>Vulnerability</b>	A flaw or weakness that can be used to attack a system or organization.
<b>Wide area network (WAN)</b>	Communications network linking computers or local area networks across different locations.
<b>Wi-Fi</b>	Wireless local area network based upon <u>IEEE 802.11</u> standards.
<b>Worm</b>	Malware that replicates itself so it can spread to infiltrate other computers.
<b>Zero-day exploit</b>	Malware exploiting a newly discovered vulnerability in a system before a patch (fix) is made available.