SECURITY

How Zap Payroll Protects Your Information

At Zap Payroll and at the third party hosting our online payroll system, keeping your data safe and secure is an important part of our business. For the purposes of this document, "We" refers to both Zap Payroll and our online payroll system provider.

How We Protect Your Information:

- We have workers whose sole purpose is to run a safeguarding program, monitoring and adjusting the program as circumstances change and they perform external security audits for critical financial applications.
- We continually perform internal risk assessments to determine and address potential risks.
- We secure our facilities, our network, and our servers.
- If we transmit financial information, we encrypt it and transmit it securely.
- We prepare for disasters to enable timely and secure recovery.
- We install virus protection on all relevant servers.
- We continually scan our network for vulnerabilities and remediate against any we might find.
- We run back-ups to a secure off-site location.
- We have an incident response plan in place should it be needed and test it on regular basis to ensure we are ready to act.
- Ensuring our workers handle your data securely
- We perform background checks on workers at hiring.
- We remove individuals' access credentials to systems and facilities when workers leave.
- We only allow authorized individuals access to information when it is critical to complete tasks for you.
- We provide training on security and privacy to all workers at hire. Workers take the security training annually and the privacy training bi-annually thereafter.

How You Can Help Protect Your Information

Create a Strong Password

Weak passwords – those that aren't hard to guess or are common words – can be easily cracked. Strong passwords are VERY important. Here are some tips for creating or changing your password:

- Use a different password for sites that contain financial information from sites that you browse casually or that don't ask for personal information.

SECURITY

- Do not use people's names and special dates as passwords. Avoid any combination of characters that friends or acquaintances can easily guess. For example, a password such as "April15" for an online tax account is NOT a strong password.
- Use syllables or acronyms. Avoid using complete words that appear in any dictionary regardless of the language. One option is to start with the first letters of a familiar phrase. For example, "Mary had a little lamb" becomes Mhall, which could be part of a secure password.
- Mix it up! Use a combination of upper and lower case letters, numbers, and punctuation/special characters, such as &^$#.
- Keep it to yourself. Do not share your personal password with others. You never know what the future will bring in relationships or coworkers, so do not give your password out – to anyone.
- Keep your passwords safe. There are programs available where you can securely store your passwords. Don't write them down in a place where others can find them.

Choose a Good User Name

Your user name is the key to your online identity on many sites. Here are some tips for choosing a good user name:

- Pick a user name that you can remember. If you create a name that's unusual for you, you may not remember it the next time you log on.
- Make it simple. Avoid using too many symbols or upper and lower case letters. It'll slow you down when you type it in.
- Never use a social security number as a user name or password. Social security numbers may be hard to guess and easy to remember, but they could give malicious hackers a coveted piece of personal information that can be exploited.
- Decide whether you want to remain anonymous. On some community sites, your user name will appear next to each of your public posts.
- Slow down. If you choose a user name in haste, you may not be able to change it later. This is especially important for accounts that stay with you for years to come.

Protect Your Computer

By using safety measures and good practices to protect your home computer, you can protect your privacy and data. The following tips will help you lower your risk while you're online.

SECURITY

Install a firewall

A firewall is a software program or piece of hardware that blocks hackers from entering and using your computer.

- Hackers search the Internet in much the same way that some telemarketers automatically dial random phone numbers.
- Hackers send electronic probes, or pings, to thousands of computers and wait for responses. Firewalls prevent your computer from responding to these random pings.
- A firewall blocks communications to and from sources you don't permit. This is especially important if you have a high-speed Internet connection, such as DSL or cable.
- Some operating systems have built-in firewalls that may be shipped in the "off" mode. Therefore be sure to turn your firewall on.
- Ensure your firewall is set up properly and updated regularly.
- Check your online "Help" feature for specific instructions.

Use Anti-virus Software

Anti-virus software protects your computer from viruses that can destroy your data, slow down or crash your computer, or allow spammers to send e-mail through your account. Anti-virus protection scans your computer and your incoming e-mail for viruses, and deletes them.

- Keep your anti-virus software updated to cope with the latest bugs circulating the Internet. Most anti-virus software includes a feature to download updates automatically when you are online.
- Make sure your anti-virus software is continually running and checking your system for viruses, especially if you are downloading files from the Web or checking your e-mail.
- Set your anti-virus software to check for viruses when you first turn on your computer.
- Give your system a thorough scan at least twice a month.

Use Anti-spyware Software

Spyware is software installed without your knowledge or consent. It can monitor your online activities and collect personal information while you surf the Web. Some kinds of spyware, called keyloggers, record everything you type in – including your passwords and financial information. Your computer may be infected with spyware if you receive a sudden flurry of pop-up ads, are taken to Web sites you don't want to go to, or if your computer begins to run slowly.

- Spyware protection is included in some anti-virus software programs.
- Check your anti-virus software documentation for instructions on how to activate the spyware protection features. You can also buy separate anti-spyware software programs.

SECURITY

- Keep your anti-spyware software updated and run it regularly.
- Download software only from sites you know and trust. Piggybacking spyware can be an unseen cost of many "free" programs.
- Don't click on links in pop-up windows or in spam e-mail.

Manage Your System and Browser to Protect Your Privacy

Hackers are constantly trying to find flaws or holes in operating systems and browsers.

- To protect your computer and the information on it, ensure your security settings in your system and browser are set at medium or higher. Check the Tools or Options menus for how to do this.
- Update your system and browser regularly, taking advantage of automatic updating when it's available. Windows Update is a service offered by Microsoft. It will download and install software updates to the Microsoft Windows operating system, Internet Explorer, and Outlook Express. It will also deliver security updates to you. Patching can also be run automatically for other systems, such as the Macintosh operating system.

Secure Your Wireless Network

If you use a wireless network in your home, take precautions to secure it against hackers. Encrypting wireless communications is the first step.

- Choose a wireless router with an encryption feature and turn it on. WPA encryption is considered stronger than WEP. Your computer, router, and other equipment must use the same encryption.
- Consider disabling identifier broadcasting if your router enables it.
- Note the name assigned to your Wi-Fi network. This name – called an SSID, or Service Set IDentifier – lets you connect your computers to the network manually. The SSID is often the equipment maker's name.
- Change the SSID on your router and the pre-set administrative password. Hackers know the pre-set passwords on many wireless routers.
- Consider turning off your wireless network when you're not using it.

Remember That Public Hot Spots May Not Be Secure.

Avoid accessing or sending sensitive personal information over a public wireless network.