EmployerUpdate

for Employers of Maine Public Employees Retirement System

MainePERS
PUBLIC EMPLOYEES RETIREMENT SYSTEM

June 2019

At This Time of Year

It is retirement plan valuation time once again. Your help is needed in order to submit timely information for our actuarial valuation. Please be sure to submit your May and June payroll filings by their due dates. If you anticipate a delay in reporting either your May or June payroll data, please contact Employer Services as soon as possible. We can be reached by phone at 1-800-451-9800 or email employer@mainepers.org.

May's Payroll Filing Due Date is:
June 17, 2019

June's Payroll Filing Due Date is:
July 15, 2019

Payroll Due Dates

Your MainePERS payroll filing "due date" is the point in time that, at the latest, a monthly filer must have both payroll information uploaded and the corresponding payment received at MainePERS. State law sets that due date as the **fifteenth day of the month following the payroll filing period being reported**. This requirement is in statute and MainePERS Rule Chapter 201, which also establishes the authority to assess interest or late charges on delinquent reports and/or payments.

Hint: Please keep in mind that you are able to upload your payroll file as early as the first day of the month following your last paid date for the payroll month being reported. Employers are encouraged to complete this upload as soon as possible after the last paid date in order to allow for adequate time to correct any issues that may arise before the last due date, which is typically the 15th of the following month.

MainePERS prefers payments be made via electronic funds transfers (EFT). EFTs are a safe, quick and convenient way to make payments. For more information on EFT submission, please contact us at 1-800-451-9800.

If you are making a payment by check, mail it along with the Remittance Report to:

Maine Public Employees Retirement System
P.O. Box 349
Augusta, ME 04332-0349

Group Life Insurance

Help your employees keep their life insurance coverage in place during the summer months. Teacher and school support employees who do not receive a paycheck over the summer must have Group Life Insurance (GLI) premiums paid during these months to keep their coverage in force. Coverage is cancelled if premiums are not paid. Employers handle this in a number of ways, with some withholding premiums due for the summer months from employee's final pay in June in order to continue remitting payments on their behalf. Other employers pay the summer premiums for their employees then withhold it from the employee when they return to work in the fall, and some employers withhold the additional premiums throughout the school year. Regardless of how you choose to withhold the premiums, please submit them to MainePERS with the monthly invoices during the summer. If you have an employee who will be responsible for paying premiums on their own through the summer, please upload a Personnel Status Change (PSC) form to MainePERS through the ESS portal indicating the employee is on a leave of absence and do an adjustment to the invoice to remove the employee from your next bill. MainePERS will then bill the employee directly for the premiums due during the summer months.

Questions?
We are here to help.
Contact us by phone: 207-512-3244 Toll free: 800-451-9800 or e-mail: Survivor.Services@mainepers.org.

Employee Contribution Rates

MainePERS realizes that many employers are right now finalizing budgets for the upcoming fiscal year. Employer and member contribution rates are effective based on the upcoming MainePERS fiscal year which begins July 1, 2019 and ends June 30, 2020. MainePERS publishes employer contribution rate information on our website. To find that information, go to www.mainepers.org, click on the "Employer" tab at the top of the page and then select Employer Home. Look to the left of this page for Quick Links and you will see where to click to get Employer Contribution Rates for State, Teacher and Consolidated PLD Employers. Grant funded teacher rate information is included in the Teacher section. The grant funded teacher costs do not include the additional amount due for teacher retiree health. This is established by and paid directly to State Employee Health and Benefits. You will receive a separate notification from Employee Health and Benefits for the retiree health amount.

Security Updates

Recently, there has been an uptick in malicious emails, worldwide. Emails are the number one vector for malicious content to enter into an organization's environment. For this reason, it is crucial for everyone to have a situational awareness about their email. Here are some reminders of how you can keep you, your organization, and other organizations you do business with, secure and free from email compromise.

1. **Email Spoofing**
   Spoofing is the term used to describe the forgery of a known sender's address with a malicious user's email address, in order to mislead the recipient.
2. **Malicious Content**
   Often times, these spoofed emails will contain attachments. These attachments can contain different types of viruses, trojans, droppers, ransomware, or other malicious code. Often this code, if clicked on and executed, can connect back to a home server to receive directions. It can download further malicious code or upload an organization's sensitive data.
3. **False Links**
   Other items in a malicious email could be a false link to a malicious site. Often times, cybercriminals will give you a false link to click on. This link could download and install similar types of content as above. Sometimes they will direct you to a website that may also be spoofed or designed to look legitimate. They often request you fill in a form with your personal information, Social Security Number (SSN), address and phone number, bank account and routing numbers, or other types of personal information.

What can you do?

First, always be suspicious of email, even if you think you know where they are from. Many times there will be grammar and spelling mistakes, or something that just doesn't 'feel' right. There will be a 'call to action,' something that creates urgency encouraging you to click or download. Don't fall for it!

1. Take a close look at who the email is from. Make sure the email address is actually the email address of the person you think it is. It is usually in the header field of your email. If it is spoofed it may say something like [Name of real person] <john.doe@fake-email.com>. If you are not sure, call the person who emailed you to verify that it is legitimate.
2. If you are not expecting an email with attached content. Don't open it. Contact your IT or Security folks to verify.
3. To detect a bad link, hover your mouse over the link. It should provide a pop-up that indicates the exact address you will be redirected to. If it is not what you expect. Don't click!

Finally, remember that we are all the front line of defense when it comes to cybersecurity. If you discover that there has been a compromise or breach, please remember that it is possible that you have also affected your other contacts and businesses with whom you have a professional relationship. Contact your IT and Security Staff. Don't forget us, please! Let MainePERS and other organizations you do business with know when you become aware of a problem. Working together we are able to help stop or slow the spread of whatever cyber infection is going around.

MainePERS thanks you!