

News You Can Use

Dec. 2013 Volume 2, Issue 2

HOLIDAY PARTIES

Keep a Lid on Alcohol, Harassment at Festivities

AS THE holiday season approaches, many small business owners will host festivities.

The goal is to keep the celebrations safe and fun.

You can achieve both goals at your office party by watching out for the following two problems: intoxication and harassment.

Alcohol

An increasing number of states require employers to exercise reasonable care to prevent injuries by intoxicated employees leaving holiday parties. To avoid many of these liability issues, an employer should lessen the role that alcohol will play during the festivities. Consider the following when planning your office party:

- Make sure the party is voluntary.
- Encourage workers to have a good

night's rest the day before the Christmas party as fatigue and drowsiness can set in much earlier when alcohol is involved.

- Use professional bartenders, and instruct them not to serve anyone who appears intoxicated.
- Distribute drink tickets to limit the number of free drinks.
- Serve heavy foods throughout the night so people aren't drinking on an empty stomach.
- Ask trusted managers and supervisors to be on the lookout for people who have had too much to drink and are unable to drive or need assistance getting home.
- Make sure employees have alternate transportation home, such as a designated driver or a taxi.
- Remind employees about any company policies on conduct and substance

abuse before the party.

Harassment

Socializing, alcohol and mistletoe can combine to create an environment that can lead to sexual harassment claims. Just because it's a holiday party doesn't mean you can't be held liable for what happens. Harassment suits can result from voluntary events held outside the office and outside normal work hours.

- Remind employees about your harassment policies before the party.
- If your business does not have an anti-harassment policy, get one. Have it reviewed by an attorney.
- Don't hang mistletoe.
- Inform all employees that they have a duty to report sexual harassment that they experience or witness.
- Finally, make sure that all employees understand that a holiday party is still a work-related activity, and that rules for appropriate work behavior still apply. ❖

Contact Us



If you have any questions regarding your coverage or our products, please call us at one of our offices:

Walnut Creek	Petaluma
San Francisco	Los Angeles
Menlo Park	Orange County
Portland	New York
St. Louis	

Sales: 877-731-7905

Service: 800-234-6787





COMPLIANCE

Ten New Laws for 2014 that Affect Your Business

AS HAPPENS at the start of every year, a wide range of new laws and regulations take effect that can have a significant impact on your day-to-day operations. Businesses have to comply with these new laws at the risk of fines, penalties or even lawsuits.

To ensure that you don't run astray of these laws, we are providing you with the top 10 new requirements you need to know about in 2014.

1. Paid family leave rights expanded – Paid family leave is mandatory in California and allows workers to take up to six weeks of paid leave to care for a seriously ill child, spouse, parent or domestic partner, or to bond with a newborn or a child recently placed through adoption or foster care. The wages are paid from a fund that is funded by deductions from all employees in the state.

The rights to paid family leave starting Jan. 1 are now extended to workers who need time to care for siblings, grandparents, grandchildren and parents-in-law.

2. Minimum wage increased – The minimum wage in California jumps to \$9 an hour starting July 1, 2014, from the current \$8. This wage applies to more than just non-exempt workers. It also applies to those working in administrative, professional and executive exemptions in California (who must earn a salary equivalent to at least two times the state minimum wage for full-time employment to qualify for the exemption).

Heads up! The minimum wage increases to \$10 in 2016.

3. Sexual harassment law expanded – This new amendment to existing sexual harassment statutes in California may end up causing confusion and additional litigation. The new law states that sexual harassment doesn't have to be motivated by sexual desire. The law was promulgated in response to a court judgment in a case where a man was sexually harassed by a male co-worker, even though his co-worker did not actually have sexual desires for the plaintiff.

4. Crime victim protections – Another piece of legislation that you need to be aware of come 2014 is SB 400, which expands existing laws that prohibit discrimination against victims of domestic violence or sexual assault to include stalking victims. The new law also requires employers to reasonably accommodate (which may include taking safety measures) victims of domestic violence, sexual assault or stalking.

Companion legislation bars discrimination against victims of certain felonies (child abuse, domestic violence, physical abuse of the elderly or a dependent adults, sexual assault, and solicitation for murder) and requires that they be given time off to appear in court.

5. Computer-professional overtime exemption hiked – The minimum compensation required to qualify for California's computer-professional overtime exemption in 2014 will be \$84,130.53 (that equates to \$40.83 an hour). If you pay them anything less than that, if they work more than 40 hours in a week, you have to pay overtime.

6. Whistleblower statute expanded – The Labor Code already prohibits an employer from making, adopting or enforcing any rule, regulation or policy preventing an employee from disclosing information to a governmental or law enforcement agency, and prohibits retaliation against employees who do, if the employee has reasonable cause to believe such information discloses a violation of state or federal law.

7. Illegal immigrant statutes expanded – Effective Jan. 1, 2014, employers are prohibited from engaging in an "unfair immigration-related practice" against an employee, such as (i) requesting more or different documents than required under federal immigration laws, (ii) using the federal E-Verify system to check an employee's work authorization status at a time or in a manner not required under federal law, (iii) threatening to file a false police report, or (iv) threatening to contact, or contacting, immigration authorities. The law allows employees to sue for relief and penalties.

Also new for 2014, employers cannot fire or discriminate against someone who updates their "personal information." This is code for someone you may have unwittingly hired who was undocumented and then later receives a green card and social security card.

8. Hazmat communications – OSHA and Cal-OSHA have required employers to train their workers in the Hazard Communication Standard.

Under the new standard, you have received new compliance labels and safety data sheets that are consistent with the United Nations' Globally Harmonized System. You should have trained your staff by Dec. 1, 2013. If not, do so now.

9. Meal and rest breaks expanded to heat illness recovery periods – SB 435 expands meal and rest break prohibitions to "recovery" periods taken to prevent heat illness. Under SB 435, an employer cannot require an employee to work during a recovery period mandated by state law under

Continues next page



SEXUAL HARASSMENT

Deadline for Prevention Training Draws Near

SINCE 2005, employers with 50 or more employees in California have been required to provide supervisors with sexual harassment prevention training every two years.

Because many companies conducted their first training that year, the end of 2013 marks another deadline for further training for those employers. Also, a new law hit the books this year that expands the definition of sexual harassment, which you need to relate to your supervisors.

If you have more than 49 employees, then you are required to conduct two hours of interactive sexual harassment prevention training for supervisors within six months of hire or promotion, and every two years after that.

You have to train all staff with “supervisory authority,” defined as anyone who has independent authority to:

- Hire, transfer, suspend, lay off, recall, promote, discharge, assign, reward or discipline other employees;
- Direct the work of other employees; and/or
- Resolve employee conflicts.

Another key portion of the law requires interactive training, meaning the session should be led by a qualified trainer and should include any or all of the following:

- Discussion,
- Role-playing,
- Question and answer session.

Topics should include at least the following to be effective:

- Teaching what is classified as sexual harassment under state and federal law.
- True-to-life examples of conduct that constitutes sexual harassment.
- Explaining what to do if sexual harassment is witnessed.
- Steps employees can take to report harassment.
- Training on what to do if an individual is personally accused of sexual harassment.
- Sexual harassment prevention methods.

Your training should also reflect changes to the definition of sexual harassment brought about by the signing into law of SB 292 this year.

That law expands the definition of sexual harassment to include conduct that is not motivated by sexual desire.

The legislation was in response to a recent Appeals Court ruling that rejected a claim by a male union apprentice ironworker who was subjected to sexually explicit comments regarding his body and threats of sexual acts by a supervisor.

The court held that since the record showed that the supervisor did not harbor a true desire to have sex with the apprentice, his abusive language and behavior could not be considered sexual harassment.

Regardless of whether you conduct the training in-house or use a vendor, make sure that you keep records of the training, the provider of the training and the date of the session for all of your supervisors.

Have everybody who is trained sign documents indicating they underwent the training.

Also, make sure that you give all employees a copy of your policies on sexual harassment, in addition to a sexual harassment information sheet on an annual basis at a minimum. ❖



Continued from page 2

Use 2014 as a Time to Prepare for the Affordable Care Act

Cal/OSHA's heat illness standard. An employer that does not provide an employee with a recovery period must pay the same premium penalty that exists for unprovided meal or rest breaks – one additional hour of pay for each workday that the meal, rest or recovery period is not provided.

Employers with outdoor places of employment are subject to Cal/OSHA's heat illness standard, which allows for cool-down periods in the shade of no less than five minutes at a time on an “as-needed” basis for employees to protect themselves from overheating.

10. Affordable Care Act prep – After the Obama administration extended until 2015 the requirement that all employers with 50 or more full-time-equivalent employees provide affordable health coverage that provides minimum

essential coverage (as outlined by the law), you should use 2014 as a time to prepare for the law, particularly reporting requirements. If you are on the cusp of the 50-employee mark (large employer), you need to carefully monitor your employee counts so that you know how to act in 2015.

Also, the IRS will start requiring that employers that provide health coverage report certain data to the tax agency. The new reporting rules have not yet been taken effect but draft rules require that “large employers” provide to the IRS information describing the health coverage provided to their full-time employees, including: the identity of those employees, the coverage offered to each full-time employee, and the months for which coverage was available. ❖



CYBER SECURITY

Half of Data Breaches Will Be Inside Jobs: Study

INSIDERS AND their actions will continue growing as a major cyber security threat to companies, according to a new study. The “2014 Cyber Security Forecast”, written by cyber security firm Kroll, predicts that almost half of data breaches will come at the hands of company insiders next year.

These breaches have largely gone unnoticed by businesses because there are typically no indications that information has been compromised. But, as the federal government and individual states beef up privacy breach notification and enforcement laws, the extent of insider attacks will become more widely known, according to Kroll.

“There’s a tremendous amount of data compromised today where the act is never discovered or disclosed,” Timothy Ryan, Kroll’s managing director and cyber investigations practice leader, said in a statement.

“People discount the insider threat because it doesn’t make the news,” he said. “Instead, we see headlines about external credit card breaches and theft of personally identifiable information, because regulations mandate accountability and punishment is expensive.”

Ryan said that countering the insider threat requires collaboration by a company’s attorney, information security personnel, and human resources.

Kroll’s report also identified other cyber security trends:

- The National Institute of Standards and Technology’s security framework and similar security frameworks will become the de facto standards of best practices for all companies. NIST recommends five core functions in keeping information and systems safe: Identify risks, protect systems, detect attacks, respond to incidents and recover afterwards.
- The data supply chain remains vulnerable. Many companies are now using third-party vendors for storing data they

collect. These contractors may or may not notify and assist you in case of a breach. Vet your contractors closely and ask about the technical and legal responsibilities of their subcontractors in the event of a breach.

- New tools help companies more quickly discover data breaches. New technologies introduced over the past year enable companies to unravel events and see with near-real-time clarity what’s happened to their data and how much damage has been done.

Having the technologies in place before a breach occurs will save you time and money if you are attacked and your data is compromised.

- The cloud and BYOD (bring your own device) movement grows, as do challenges for companies. Companies’ IT departments are working overtime to get in front of the dangers posed by cloud storage and employees using their own smart devices to access company data. Your management needs to work closely with your IT department and legal counsel to adapt policies that addresses changing legal risks.

“We’re seeing courts issue rulings that include significant penalties where discovery, disclosure and other legal obligations aren’t being met because of the use of these technologies,” said Alan Brill, senior managing director at Kroll.. “Companies that have integrated these technologies into their corporate policies, IT security, and risk management plans will be much better prepared to fulfill their legal obligations.” ❖



Reducing Cyber Coverage Costs

YOU CAN reduce the cost of a cyber liability policy by using best practices to safeguard your data and by reinforcing your security practices before you apply.

This should include:

- Password management. There are affordable password management solutions.
- Conducting regular risk assessments to reveal hardware, software and individual site vulnerabilities.
- Creating a written IT security policy that identifies critical assets and defines policies for physical security, account management, and backup and recovery, among other areas.
- Leveraging firewalls, virtual private networks, anti-virus and anti-spam software and securing mobile solutions to secure network access and mobile devices.



Produced by Risk Media Solutions on behalf of Heffernan Insurance Services. This newsletter is not intended to provide legal advice, but rather perspective on recent regulatory issues, trends and standards affecting insurance, workplace safety, risk management and employee benefits. Please consult your broker or legal counsel for further information on the topics covered herein. Copyright 2013 all rights reserved.