FAIR MEASURES, INC.

P.O. Box 2146 Santa Cruz, CA 95063
831-458-0500, fax 458-0181
www.FairMeasures.com
training@FairMeasures.com

Managing Within the Law II

reference materials

We gratefully acknowledge the contributions to these materials of all of the attorneys who have worked with Fair Measures: Rita Risser, J. Logan, Jonathan Levy, Ann Kiernan, Steve Duggan, Lynne Eisaguirre, Julie Crane, Joelle Sullivan and Michele Huff. We also are grateful to our clients, and their legal counsel, Human Resource professionals and Training Department staff, who have given freely of their ideas to improve this course.

Managing in Cyberspace

Nearly 50 million people – one third of all U.S. workers - reported that they teleworked in 2008. These workers include regular telecommuters, frequent travelers, employees on part-time schedules, individuals on family or medical leave, and people needing reasonable accommodation for disabilities. Field offices are full of sales people, service personnel and consultants who hardly ever see the "real" office. At many companies, a manager may be time zones or even continents away from the staff.

Modern managers must be equally adept handling the employees they see once a calendar quarter and those they see every quarter-hour. Traditional management, which relies heavily on face-to-face conversations and observation, won't work in cyberspace.

Successful remote management is based on mutual trust and excellent communications. Both you and your cyberspace employees should be clear speakers and accurate writers, as well as good listeners and careful readers. Here are some practical tips:

- ✓ Make planning and scheduling replace relying on "bumping into someone" in the office
  --Help teleworkers organize their assignments and set timetables and goals
  --Ask for feedback about work conditions, challenges, and how you can help

- ✓ Regular electronic communication will become your informal conversation/contact
  --Consider using instant messaging or e-meeting software
  --Try to "stop by" via e-mail or telephone--every day, if possible
  --Respond to e-mail/voice mail from teleworkers quickly

- ✓ Remember to include teleworkers in meetings, both the big ones and the small brainstorming sessions.
  --Make sure teleworkers are included in conference calls
  --Videoconferencing can make collaboration easier and more productive

- ✓ Resist the urge to give assignments just to the people you see every day.
  --Out of sight should not be out of mind!

- ✓ Switch to results-based management.
  --What's important is the final product, not how much face time someone puts in.

Of course, when work leaves the office for home, the field or a drop-in office, employment law goes along. There are three key questions you should ask yourself:

- How do I apply these laws to employees in cyberspace?
- How can I ensure that I am treating remote employees consistently with local employees?
- What systems should I put in place to let remote employees know their rights and responsibilities?

Hot Topics in Cyberspace Employment Law

Here are some hot areas to keep in mind:

Americans With Disabilities Act

The ADA never mentions working from home or another remote location as a reasonable accommodation for a disabled worker. In a 2003 policy statement, the EEOC said that while the ADA does not require an employer to offer a telework program, it must allow employees with disabilities an equal opportunity to participate in any such program. It appears clear that telework is not appropriate when the employee's essential functions require regular time in the office, or when the employer would suffer an undue hardship. But, the courts are evaluating these issues on a case-by-case basis.

Of course, a manager cannot require or forbid a disabled employee to telework, unless that is also required or prohibited of similarly-situated able-bodied workers. When selecting teleworkers, managers should use consistent, job-related criteria such as reliability, organization skills, discipline, and self-motivation.

Family and Medical Leave

Sometimes, telework can be a good supplement or alternative to FMLA leave. The employee can keep working (on a reduced schedule) while attending to family and medical needs. But be careful about telework as a solution to child- or dependent-care needs. Both parties are responsible for insuring that the employee's personal obligations do not interfere with effective, quality work.

Workers' Compensation

Under state Workers' Compensation laws, an employer is responsible for injuries to an employee while working. Since managers cannot physically supervise cyberspace employment, this presents some unique legal complications:

Injuries that happen in the office, factory or other company facility are presumed to have been caused by work. But, injuries at home must arise out of and in the course of employment, not out of "personal frolic," to receive workers' compensation.

Does the employer have to inspect a home office? Does a home office have to comply with ergonomic, electrical, and other safety standards? While OSHA has abandoned the position that it has the same jurisdiction over home offices as it does over the traditional ones, employers still have the obligation to provide a safe workplace. Employers must balance that obligation with employee privacy concerns.

What about fraudulent claims? Unlike injuries in a traditional office, store or factory, there will rarely be witnesses (other than a pet or family member) when a teleworker gets hurt. The company must rely on the worker to report accidents promptly and accurately.

Performance Management and Promotions

Traditionally, supervisors and managers relied on direct observation of employees to learn how well they did their jobs. Of course, that's not possible in cyberspace. Rather than rely on what they see, managers can be guided by clues such as the time it takes a direct report to respond to an e-mail, or to return a telephone call to colleagues.

What is possible—and preferable—is to focus on results and productivity. Managers have to figure out how to measure the quality of the work done remotely, as well as the number of projects or tasks completed.

With teleworkers as with all employees, it is crucial to set clear performance objectives. Both manager and employee should agree on specific tasks and objectives to be accomplished during a specific period of time. There should be mutual understanding of which tasks are critical, and which can be put on the back burner, if need be.

When considering employees for promotions and training, out of sight should not be out of mind. Companies that post all internal job and training opportunities on the web are treating remote workers consistently with those in the office. Managers should encourage remote employees to apply for appropriate promotions, and give them due consideration.

Wage and Hour

Non-exempt employees in cyberspace present another challenge: accurate time-keeping. Even when a company cannot physically monitor a teleworker, it is still legally responsible for paying wages for all time worked. Managers must rely on non-exempt remote employees to record their weekly hours and any overtime. Under the law, even if employees work unauthorized hours, they still must be paid for them, with overtime, if required.

In the first court decision on the subject, New York's highest court ruled in 2003 that a telecommuter was eligible for unemployment benefits only in Florida, where she lived, and not New York, where the employer's place of business was located. The Court of Appeals reasoned: "In our view, physical presence is the most practicable indicum of localization for the interstate telecommuter who inhabits today's 'virtual' workplace linked by Internet connections and data exchanges."

Illegal Harassment and Discrimination

Most employees view the opportunity to work at home as a big plus. A worker who has asked to telework and has been denied that privilege may allege that the manager unlawfully discriminated in refusing to offer the opportunity. At least one federal appeals court has recognized that denying telecommuting privileges may be an "adverse employment action" when considering a discrimination and retaliation claim.

To avoid such claims, make sure you follow all company guidelines for selecting teleworkers. You should be able to document that you made your decision based on legitimate, job-related and non-discriminatory standards.

Even though a teleworker is off-site, all the laws on discrimination and harassment apply, just as if the worker were in the office.

A 2006 New Jersey appellate case alerts managers to their responsibility to prevent crimes on company property. The case was brought by a woman who had a 10 year old daughter. The woman had

recently married a man who was employed by "XYZ Company." About six months after the wedding, the woman realized the man had been taking inappropriate photos of her daughter and posting them on the web. She discovered he had been posting from his computer at work.

The woman sued the company for allowing the man to use his computer at work for illegal purposes, without reporting him to the authorities. A number of people at XYZ Company knew he was visiting inappropriate sites, including the manager of Information Services, his supervisor and manager, and the head of Human Resources. Nonetheless, he had received only two verbal warnings to stop.

The court held the company had a duty to report him, and allowed the woman to go forward with her claim against the company.

> ***practical pointers:*** If you know of illegal web surfing by employees, it is your duty to report it to management, and ultimately to the police.

Intellectual Property

Teleworkers often have access to the company's computer system from remote locations, as well as to hard copy files and documents in their home offices, drop-in centers, etc. Obviously, confidentiality agreements, passwords and other security measures are essential. When a teleworker is terminated or the telework arrangement ends, the employer should immediately change passwords and retrieve its computer, office equipment and files.

Teleworkers should know that any patents, trade secrets or other intellectual property they develop while working belong to the employer, even though they were created at the employee's home or other remote location.

A teleworker's unauthorized use of software on the employer's computer could lead to employer liability for copyright infringement or license violations, so make sure all software given to a teleworker is properly licensed for that use, and forbid teleworkers from using any non-authorized software.

Any hard copy information that would be shredded in the office must be shredded by the employee at home, or brought in to the office for shredding. The employee must ensure that no one else at home (e.g. spouse, roommates, domestic partner, children) has access to the

computer or hard copy information that is company confidential. If employees also work at home for a competitor, they cannot use company-provided equipment in the service of that competitor, nor can they put company confidential information on any machine that also has information from the competitor.

Privacy

Managers should be aware that U.S. Customs officials have the power to seize and search the contents of any laptop computer being brought into the United States, as a routine border search. There does not have to be any reasonable suspicion or probable cause. This power was upheld in a 2006 federal appeals case.

Employers with operations in the European Union (EU) have to be careful to not violate the EU's strict privacy restrictions on employee information. Under EU rules and implementing legislation in its member states, "personal data" is defined very broadly, and includes "any information relating to an identified or identifiable natural person." Employers can use personal data only for specifically defined purposes, including administering payroll, performing an employment contract, and assessing performance. Employers have to give employees notice of the collection and use of personal data, and there are civil and criminal penalties for non-compliance.

Managers in the US who supervise EU workers should be aware that EU rules forbid transferring employee personal data to countries without "adequate" privacy protections. From the EU's point of view, the lack of national privacy laws in the U.S makes its data privacy protection rules inadequate. But the EU and the US Department of Commerce negotiated a "safe harbor" agreement in 2000, under which U.S. companies who agree to abide by the safe harbor principles and certify to the Department of Commerce that they are in compliance will be allowed to transfer personal data on European and expatriate employees from Europe to the United States.

If you are dealing with EU employees, make sure you find out what you need to do to protect their privacy rights.