MICHIGAN CATHOLIC CONFERENCE

Risk Management Services

THE RISK MANAGEMENT REMINDER

Fall 2006

EMPLOYMENT PRACTICES

What has cost you and your (Arch) Diocese nearly $1,000,000 in the past 40 months? Employment Practices Liability claims and lawsuits. These developing claims are currently reserved at over $1,300,000. Prior analysis of these costs show that these reserves can increase up to 70% in as little as 24 months. It is possible that this reserve could reach $2,200,000 in the coming months.

There are literally hundreds of laws, both state and federal, dealing with employment practices. These laws range from the Family and Medical Leave Act (FMLA), to all elements of harassment to the Uniformed Services Employment and Reemployment Rights Act (USERRA) to protected classes of employees to alleged wrongful termination. These evolving laws have sparked numerous claims by employees against their employers; and we have not been exempt from this national trend.

It would be impossible to list all the do's and don'ts of employment practices. Likewise, the ever-changing legal aspects require the use of experts to help you with employment practices questions. Each of your (Arch) Diocese has personnel policies and procedures. Most are available on your respective websites. Please use these resources when hiring a new employee, and consult with your (Arch) Diocesan contact on any proposed lay-off, termination or demotion. This will ensure that you are in compliance with the laws and help protect you from a future lawsuit.

Protecting yourself from employment related claims begins with the hiring process and use of (Arch) Diocesan resources throughout the employment relationship. Although the resources may vary, the basic elements are consistent and include the following:

Continued inside

Please share this Newsletter with your staff.

ROUTING:

- ❒ Pastor
- ❒ Associate Pastor
- ❒ Administrator
- ❒ Bookkeeper
- ❒ Principal
- ❒ Director of Religious Education
- ❒ Director of Youth Ministry
- ❒ Athletic Director
- ❒ Maintenance Staff

New Employee Checklist

- Job Description
- Employment Application
- Form I-9 (Immigration)
- Form W-4 (Withholding)
- Personnel Policy
- Acknowledgment Form(s)

Employee Termination Checklist

- Letter of Resignation
- Status Change Form
- Exit Interview
- Last Paycheck with unused vacation
- Equipment and key return

Not all Employment Practices Liability claims result from terminating or demoting employees. Co-worker complaints of harassment by another must be reviewed and investigated. Workers' Compensation (WC) claims require immediate reporting for handling within the act covering benefits under WC coverage. Complaints of discrimination, race, sex, national origin, age, etc. must be handled in consultation with your (Arch) Diocesan resource. A couple things to keep in mind are: document employee behavior, including absenteeism or tardiness, unsatisfactory performance, noting reprimands and disciplinary action and do not overlook inappropriate behavior and allow it to permeate the workforce as this can lead to harassment charges if not kept in check.

If you detect that a claim is to be made by a disgruntled employee, immediately contact your (Arch) Diocesan resource and our claims administrator, Gallagher Bassett Services, Inc. (GBS). Likewise, should a lawsuit, Michigan Department of Civil Rights, or Equal Employment Opportunity Commission inquiry be served on you, contact your resource and GBS.

COMPUTER AND DATA SECURITY

In the age of ever-advancing technology, computer crimes such as identity and data theft have become commonplace. One way that many parishes are taking advantage of today's technology is allowing their parishioners to setup automatic withdrawals for their weekly giving. Most of our schools also keep records of their students and their guardians on some form of an electronic database. Social Security numbers, bank information, address and contact information, as well as other personal information are examples of what is stored on parish and school computers. This data needs to be protected from unwanted access. Several security measures must be in place to ensure the privacy of this very personal data. Some things to keep in mind are:

- Keep your operating system updated. Regularly check your operating system and download updates that may contain security patches and fixes for your PC.

- Install a firewall. Unprotected, a Windows computer will most likely be infected within 30 seconds to 5 minutes of connecting to a high-speed network. A firewall is a system that prevents unauthorized access to your network and/or computer, and is your first line of defense in protecting private information and data.

- Use anti-virus and anti-spam software. A good anti-virus/anti-spam program will protect your computer against spyware, adware, malware, and other Internet threats. Remember to update them regularly.

- Install pop-up blockers. Pop-ups serve little purpose, are annoying, and are typical ways for unscrupulous hackers to gain control of your computer.

- Beware of email messages. Never open emails from people you do not know, or respond to email requests to validate financial information. Most importantly, do not open any attachments until they have been scanned by anti-virus software.

- Use secure passwords. Do not use names of people, pets, places or personal information for passwords. Refrain from using words found in the dictionary. Passwords should be creative containing random characters and numbers, at least 6 characters in length (longer is better), and changed monthly.

- Do not store vital information on the computer. Rather, use floppy diskettes, compact discs, or pen drives to store sensitive data. Lock them up when not in use.

- Encrypt sensitive data when transmitting over the Internet. If you exchange sensitive data with your (Arch) Diocese or financial institution, encrypt the information prior to sending it.

- Shred discarded documents. Buy a personal crosscut shredder and shred all disposed documents that contain sensitive information.

- Protect your wireless network. Disabling SSID broadcasting will prevent hackers from "listening in" on computer transmissions.

- Perform regular backups. Routinely backup your computer's hard drive and store the backup in a safe (and preferably offsite) location. Make sure you test your backups occasionally.

- Implement acceptable use policies. Defining the appropriate use of computers provided by schools, parishes, etc. will reduce risk and help minimize the loss of sensitive information.

No amount of security can guarantee against theft and tampering but it can make it extremely difficult. It is your obligation as schools, parishes, etc to protect the data you store and access, so you need to put as many security measures in place as possible. If you have any questions regarding data and computer security, please contact the Information Systems and Services (ISS) department at Michigan Catholic Conference (1-800-395-5565).

LABOR LAW POSTINGS

The new labor laws and hourly rates are currently being finalized for the State of Michigan. These will be posted to our website, www.micatholicconference.org, in our Gateway section. Within the Risk Management section, you will find a link called "Risk Management Info. & Forms" where the Labor Law postings are available. You may download the forms and posters directly from the website and post in your workplace accordingly.

LOSS PREVENTION REMINDERS

All injuries, losses, claims or damage require immediate reporting to our claims administrator, Gallagher Bassett Services, Inc. They will provide the initial direction to reduce the loss exposure, if possible. For the Archdiocese of Detroit, phone 248-352-1062, fax 248-350-1710. For the Diocese of Gaylord, Grand Rapids, Kalamazoo, Lansing, Marquette and Saginaw, phone 1-800-926-1819 or 517-351-3100, fax 517-351-5528.

Michigan Catholic Conference
510 South Capitol Avenue
Lansing, Michigan 48933

NONPROFIT
U.S. POSTAGE PAID
LANSING, MI
PERMIT NO. 35