



Privacy: What you can do to protect *OUR* information

Increasingly in recent years, universities have become the targets of hackers and identity thieves. Experts in the areas of privacy and data security have reported that more than a quarter (and possibly as high as a half!) of the data breaches that occur these days involve universities and other educational institutions. The reason: Universities are known for having open networks and data systems that focus more on collaboration and the free exchange of ideas rather than data security.

To help us comply with the various privacy and data security requirements out there (and the ones still to come!), the University has implemented several policies and procedures that outline what we, as University employees, must do to help the University ensure compliance and safeguard personal information. The University is also in the process of implementing additional initiatives and policies and launching additional training to ensure that we keep only the data

that is required to be kept, that we properly protect the integrity and security of the records we do need to keep, and release only what is required to be released by law and in accordance with University procedure.

Remember, as a University (and a State) employee, much of *your* personal information is also included in University data systems. We all want our personal information to be protected. **So what can you do to help?**

- If you are a faculty or staff member who taught students or otherwise worked with student data when Social Security Numbers were used as ID numbers instead of, or in addition to PeopleSoft numbers, review your files or run a scan of your computer to determine if you have files that contain Social Security Numbers. You should do a similar review or scan if part of your job requires you (or previously required you) to collect and/or use social security numbers, credit

card information or driver's license information. UITS has software that can help you run these types of scans.

- If you do have Social Security Numbers, credit card information, driver's license information or similar personal data on your computer, ask yourself the following questions: Do I still need to keep this information? Why? What purpose does this data still serve? What do the Connecticut or Federal record retention laws require? (call the University's records retention liaison, Betsy Pittman with any questions). Where else might this data be housed at the University such that I do not need to keep a copy of it?

(Article continued on page 3)



The "Compliance courier" is a quarterly newsletter issued by the Office of Audit, Compliance & Ethics. For questions or concerns, please contact Kimberly Fearney at (860) 486-6195 or Kim.Fearney@uconn.edu.

Meet the Compliance Staff

The Compliance area of the Office of Audit, Compliance and Ethics includes both familiar and new faces to the University. In a continuing effort to help familiarize employees with the Compliance Office, below is a brief description of each staff member's role and how they came to call UConn home!

Rachel Rubin—Rachel received her undergraduate degree from the UConn Business School. Rachel returned to the University after serving as Managing Director and Commission Counsel for the former State Ethics Commission and as compliance counsel for a private company. Rachel has also served as advisor to Governor Rell on ethics compliance and public integrity issues. Rachel currently is the Director of Compliance for Storrs and the Regional Campuses.

Kimberly Fearney—Kim is a graduate of UConn's College of Liberal Arts and Sciences. Kim started her professional career at UConn in the Department of Human Resources before moving to the OACE in 2006. Kim develops and presents the annual compliance training, oversees the E-Policy webpage as well as conducts REPORTLINE investigations.

Rachel Krinsky Rudnick—Rachel is a graduate of the UConn Law School. Before returning to UConn in 2006 as the University Privacy Officer, Rachel worked as a private attorney. Rachel oversees matters relating to privacy of employee and student information, coordinates the University's responses to Freedom of Information (FOI) requests and conducts REPORTLINE investigations.

Elizabeth Vitullo—Liz graduated from Fairfield University with a B.A. in English and is currently pursuing her graduate degree here at UConn. Prior to joining UConn in 2007, Liz worked for the City of Hartford. Liz is responsible for assisting with FOI Requests, investigations and Compliance Training.



Pictured: Liz V., Rachel K., Rachel R. and Kim F.

REMINDER

Compliance Training sessions are scheduled to begin soon!

Stay tuned for further announcements.

REMINDER

REPORTLINE Update

As reported in our Fall 2007 issue, The Office of Audit, Compliance and Ethics launched the University's confidential compliance reporting system, the *REPORTLINE*, in June of 2006. Although the allegations reported and actions taken remain confidential, our office feels it is important to periodically update employees on the effectiveness of the *REPORTLINE* and educate on "lessons learned".

We have received 41 initial reports through the

REPORTLINE in the last twelve months. Many reports include allegations of University policy violations as well as misuse of state resources. Examples include using state resources, including vehicles, for personal use and violations of posted policies by University departments. Although many allegations are found to be unsubstantiated, these can serve as helpful reminders for employees and departments regarding what you should and should not do in the course of your job.

Regarding personal use of University resources, it is

important to remember that more and more people are watching what we do as "public employees." Please make sure any use of University property is for business purposes only.

Regarding policy, always check with the appropriate authority regarding legal and statutory references before publishing policies. Laws change frequently, and departments may find their policies are contradictory with applicable laws.

Please stay tuned for further updates on the *REPORTLINE* in future issues.

Privacy continued ..

If you know you have (or even think you might have) sensitive or personal data on your computer, consider what steps you and/or your department have taken to protect that information. Is it backed up on the server? Are the files individually encrypted? Is your computer whole-disk encrypted? Is your computer and/or the individual files on the computer password protected? Do you "lock" your computer when you get up from your desk with password protection? Do you shut down your computer when you leave for the day? Is your office or work area locked?

These are just some things to consider. Even if you took all of the steps above, you might not be able to ensure with 100%

certainly that personal information or other sensitive University data or University systems will not be compromised. However, if each University employee takes steps to protect the data they have on their computers or in their offices to the best of his or her ability, we will be well on our way to ensuring that we are not among the Universities who face legal action and negative publicity when a data breach occurs.

If you have questions about complying with privacy and data security requirements, please contact Rachel Krinsky Rudnick at 486-5256 or rachel.krinsky@uconn.edu.

**Coming Soon:
Take the
Compliance
Office Survey!**



UNIVERSITY OF CONNECTICUT

OFFICE OF AUDIT, COMPLIANCE & ETHICS

9 Walter's Avenue, Unit 5084
Storrs, Connecticut, 06269-5084
Telephone: (860) 486-4526
Facsimile: (860) 486-4527

Web: www.audit.uconn.edu

REPORTLINE

Phone: 1-888-685-2637
Web: [www.compliance-helpline.com/
uconncares.jsp](http://www.compliance-helpline.com/uconncares.jsp)

POLICY CORNER

The following policies were recently posted on the E-Policy website. Each policy is either a new University policy or an update of an existing policy. For questions regarding any of these policies, please refer to the contact information listed on the E-Policy website.

Compliance Training Policy

The University is required to provide all employees and related parties with annual training on the elements of the compliance program and the University's expectations that all will act in accordance with applicable laws, policies and standards.

Driving and Motor Vehicle Policy

The purpose of this policy is to set forth the requirements applicable to all drivers of UConn owned, operated, leased and/or rented vehicles when in the course of conducting official University business.

Emergency Closing Policy 2008-2009

The purpose of this policy is to provide the protocol whereby University officials may declare a late opening, early release or shut down for an entire workday, all or a portion of the University and shall communicate this information to employees.