



## University Compliance **Helpline**

The University of Louisville is serious about fostering an atmosphere of integrity and honesty. It is everyone's responsibility to adhere to and comply with laws, regulations and policy on the University's behalf. UofL's new Compliance Helpline is a simple way to report activities that you suspect are unethical violations or criminal. The Helpline is operated by an independent company hired by UofL's ICO (Institutional Compliance Office) to ensure that our compliance reporting is objective.

The Compliance Helpline is an effective way to report activities via the toll-free number below. UofL employees may also submit a report online at the "Compliance Helpline Reporting" option on ULink.

### 1-877-852-1167

Call 24 hours a day, 7 days a week.

When you witness activity that may be questionable, please let us know by calling the Compliance Helpline. This could be anything related to:

- research
- information security
- financial transactions
- environmental
- medical practice
- privacy
- human resources
- health & safety
- athletics
- and more

This service is not a substitute for, nor does it supersede, any existing reporting methods or protocols already in place at the University of Louisville for reporting suspected problems or complaints. Instead, the Compliance Helpline provides an additional means of reporting such issues.

For more information, please visit the ICO website at <http://louisville.edu/compliance/helpline> or call the ICO at 502-852-8305.

*When in doubt,  
point it out*



## **GOT COMPLIANCE?**

**Mere knowledge of the rules is not enough.**

The U.S. Sentencing Commission, an independent agency in the judicial branch of the federal government was organized in 1984 to develop national sentencing policy for federal courts and first promulgated "sentencing guidelines" in 1991 to structure federal courts' sentencing discretion to ensure that similar offenders who commit similar offenses receive similar sentences. These guidelines identify seven minimum requirements of an effective compliance program and provide incentives for organizations (including universities) to create meaningful compliance and ethics programs. Significant amendments to these guidelines in 2004 expanded the definition of an effective compliance and ethics program beyond the exercise of due diligence to prevent and detect criminal conduct to include that an entity must promote an organizational culture that encourages a commitment to compliance with the law. The following are the seven elements of an effective compliance program addressed in the guidelines found at [www.ussc.gov](http://www.ussc.gov).

1. Adequate compliance standards and procedures;
2. Effective compliance oversight;
3. Careful delegation of authority and due care in hiring/screening employees;
4. Effective training and education for roles and responsibilities;
5. Monitoring, auditing, and hot lines;
6. Enforcement for violations; and
7. Corrective action.

UofL's compliance program continues to evolve to provide assurance that the institution is complying with internal and external laws, regulations, policies and procedures as the University moves forward to become a nationally recognized premier research university. Please visit the new Institutional Compliance Office's website at <http://louisville.edu/compliance> for a directory of University compliance contacts /departmental subject matter experts.

## The Information Security Office

### *What is the Information Security Office?*



The University of Louisville Information Security Office (ISO) oversees information security policies, standards, evaluations, compliance and university-wide security awareness and is managed by Bruce Edwards, UofL's Information Security Officer. The ISO is part of the university's overall compliance program and coordinates information security efforts and activities across the university including InfoSec strategies and global function oversight as well as coordination of security efforts related to student, employee, patient and other sensitive information.

#### **Some ISO activities**

The ISO has played a key role in heightening information security awareness and appreciation at all levels of the University, working with senior University management as well as organizing a very popular annual Cyber-Security Awareness week now in its third year (the week of October 1, 2007 this year – watch UofL Today for announcements, including free cook-outs on Belknap and HSC!).



The ISO spearheaded the reorganization and rewriting of the University's Information Security policies and standards which required general consensus among numerous diverse stakeholder groups and focusing on a common foundation for InfoSec compliance. The "common foundation" approach was selected because the:

- **Laws, regulations and requirements** (HIPAA, PCI, FERPA, NIH, contracts, federal and state legislation, etc.) and
- **Expectations** of sponsors, donors, collaborators, our constituents, media, the public

#### **Ask the Auditor ...**

Do you have a question about business practices, controls, frauds, computer security, or a related matter? We will publish selected non-confidential questions and responses in future "Ask the auditor" features. We look forward to hearing from you. Please call us or send us an e-mail.

in numerous areas are similar. Therefore a unified approach is more efficient, effective and less confusing. The policies and standards were approved on July 23, 2007 by the Compliance Oversight Council, the University's executive level compliance oversight body.

With regards to general Information Security at UofL, the ISO focuses on four areas:

1. Risk Assessment and Management – Communicating information security risk to the Institutional Compliance Officer, the Compliance Oversight Council and others within the university; recommending appropriate mitigation activities or risk acceptance;
2. Education in the form of training, awareness efforts and consulting;
3. Improving compliance using consulting, auditing and monitoring, assessment and adjustment or mitigation;
4. Maintaining policy relevance using self assessment/audit, feedback and adjustment.

The ISO offers consulting on Information Security requirements at UofL to all departments and also represents the university in the community and state-wide by advising on security issues to the Louisville Health Information Exchange and to the Kentucky e-Health Network Board.

#### **Classified and Sensitive Research**

The ISO is also transitioning into somewhat similar additional responsibilities related to the administration and management of federal requirements related to classified research, sensitive but unclassified research and export controls. The classified aspects of these functions are handled by the "Facility Security Officer" or FSO (the Federal Government's nomenclature), so once Federal Government clearances are processed, the ISO will also be the University's FSO. The FSO should not be confused with the Department of Public Safety (DPS) which continues to handle policing and other safety duties.

**More information is at the ISO web site:**  
[security.louisville.edu](http://security.louisville.edu)

#### **How to contact us:**

Our web site –  
<http://louisville.edu/vpf/audit/index.html>  
Fax – 502-852-0740 Phone – 502-852-8305  
E-mail – [intaudit@gwise.louisville.edu](mailto:intaudit@gwise.louisville.edu)  
Audit Services, University of Louisville,  
1900 Arthur Street St. 300, Louisville, KY 40208-2769