

Shaun King and Dorothy K. Robinson

From: Shauna King and Dorothy K. Robinson
To: Business Managers and IT Support Providers
Sent: October 17, 2007
Subject: Removal or Encryption of Electronic Restricted Data

Following recent thefts of administrative and academic computers, including two from the Yale College Dean's Office that held a large number of Social Security numbers, we asked Information Technology Services to sample additional machines for legally restricted data. That sample suggests that many Yale computers may hold restricted data, and, in many cases, the data may no longer be used and may be unknown to the machine's user. Because of Yale's responsibility to protect student, alumni, faculty and staff data, we have asked Philip Long, University CIO, and his staff immediately to plan and implement a campus-wide project to remove or encrypt restricted data stored on Yale-owned desktop and laptop computers or other media.

Changes in institutional systems over the last several years allow us to accomplish most university work without using restricted data such as Social Security numbers or credit card numbers. At the same time, unauthorized releases of those data not only have the potential to harm individuals but also carry costly and burdensome legal consequences, such as the requirement to identify and give notice to all persons affected by an inadvertent breach of security. For these reasons, we have determined that faculty and staff should continue to store legally restricted data on Yale owned desktop and laptop computers or portable media *only where it can be specifically justified as essential for current operations. In such case, encryption and other security measures must be employed.*

Stewardship of University electronic data is a shared responsibility of the staff or academic client and that client's IT partner. We are calling on you as members of the business leadership and IT support communities to assist your department and the University to safeguard the legally restricted personal data of faculty members, students, staff and alumni. To assist Business Managers, Phil Long will be working with Steve Murphy, Associate Vice President for Business Operations, and his business operations team to coordinate the remediation process to ensure we address distributed data security issues in a manner that complies with the law and recognizes the complexity and challenges of Yale's operations. To assist IT support providers, Phil Long will shortly ask those of you serving specific schools or departments to attend an overview of the distributed data clean process. ITS will conduct the session and provide detailed explanations of the process and the coordination required to reduce your department's distributed data risks. We ask your cooperation as business managers and IT support providers in working with ITS to plan and manage these data cleanup efforts in your areas of responsibility.

As a first step, we have authorized ITS and, under ITS established procedures, local staff to conduct a focused scan of computers in order to discover and remediate Social Security numbers and credit card numbers. This work will be conducted in accordance with the Information Technology Appropriate Use Policy that applies to all members of the Yale community (faculty, staff, students and network visitors; <http://www.yale.edu/ppdev/policy/1607/1607.pdf>) and will include the full engagement of IT support staff across the University. Work will begin with the administrative offices most likely to have such residual data but, ultimately, is planned to extend broadly across the campus.

The scan will seek only Social Security numbers and credit card numbers and will be designed to protect user privacy to the greatest extent possible. Information about how this process will work is available at www.yale.edu/its/secure-computing/data-faq.html including basic instructions for how clients might begin this work on their own.

The University has discussed this project with the agencies investigating Yale's grant management practices, and we have identified persons who will not be participating in the project because they may have documents related to specific grants under review. In addition, this project does not override the University's other legal obligations to preserve records (for example, tax records, medical records, certain personnel records, and current research records). Should you or your departmental colleagues be uncertain about whether or not you can delete information, please wait to take action until the project team contacts your department. The team will arrange appropriate advice on these decisions at that time.

Your cooperation and assistance in the coming months with this effort is essential to ensure success in this important work. Thank you in advance for your assistance.