March 30, 2011

To: Cornell University Library Staff  
From: Anne R. Kenney, Carl A. Kroch University Librarian

The misuse of confidential computer data to steal identities and violate privacy is a serious and ongoing problem. Over the years, Cornell has been entrusted with extensive confidential information on our faculty, staff, students, and alumni. It is our shared responsibility to ensure that this data is secure and protected against exposure and loss.

This past December, President David Skorton initiated a university-wide effort to clean up and inventory confidential data held on computers used by Cornell faculty and staff. Last week, CIO Ted Dodds sent out a follow-up memo expanding on the President’s directive. Quoting from that memo:

> Simply put, Cornell needs to better protect electronically stored information, particularly the personal data that students, employees and other people associated with the university have placed in our care. The increasing frequency and sophistication of attempts to inappropriately or illegally access sensitive information - and the growth in regulations covering electronic data - demand that we reduce the risk of data breaches and the significant financial and regulatory losses they bring. Over the past few years, Cornell has experienced a number of incidents where institutional information has been compromised or lost. One of our major weaknesses is that, like most universities, sensitive data is scattered throughout the institution. Often that information is no longer needed and/or forgotten.

In taking care to prevent compromise or loss, we must think about how and where we store confidential data and take steps to make sure that it is protected. Surprisingly, two thirds of computers examined across a wide array of institutions, including Cornell, have some legally protected data stored on them. Most computer users are unaware of confidential data on their computers, and almost none of the data is stored securely.

To protect this data, we must examine the computers in our care, determine where confidential data exists, delete unnecessary data, and properly secure the data that we must retain.
I have asked Dean Krafft to lead the Library’s data cleanup effort. He has been working with Library HR and IT staff to put the processes and tools in place to support this effort, and we have already begun some initial pilot efforts within the Library.

I am asking you to clean up all computers and data storage devices under your care. This isn’t a job that can be delegated to someone else, because it involves examining your files and deciding which files to keep. If your work does require that you keep confidential data, then there will be additional steps to inventory and secure that data. There will be computer tools, documentation, and assistance available from Library IT staff and CIT to help you in this effort. You can find extensive information on this entire initiative at http://www.cit.cornell.edu/datacleanup/.

This is a massive effort, which President Skorton has asked us to complete by June 30, 2011. Library IT and HR staff will be contacting department heads and supervisors to roll out the tools and processes. Once that is done, I will need a statement from each of you certifying that:

• You take responsibility for the data on devices used for university business that are under your control.

• You are taking appropriate steps to understand all confidential data in your care and properly secure any confidential data retained.

These attestations will be collected from Library staff by a web tool being created for this purpose.

Given the impact of the loss or exposure of confidential personal data both on the individuals affected and on the reputation and financial resources of Cornell University, I am asking each of you to join in this effort and to do your part to secure all confidential data in our care.