Division of Information Technology
University of South Carolina

SecureCarolina DLP Spotlight

Data Loss Prevention (DLP) technology allows the university to protect itself from data breach while also protecting user privacy.

What is DLP, and Why Do We Need It?

In today's world, data breach and identity theft are often at the forefront of information technology (IT) discussions. That's why more laws and policies are being used to govern computing. Consequently, following the South Carolina Department of Revenue breach, the Board of Trustees approved the SecureCarolina project, a university initiative to greatly improve information security at the University of South Carolina. It is much simpler to take the necessary steps to protect the data before a costly and embarrassing breach occurs.

The University Information Security Office has been charged with "the responsibility to develop the university-wide Information Security Program" in IT 3.00. Policy UNIV 1.50 engages users, requiring that they "protect their data access privileges and the data they are entrusted with, according to established University Policy, Standards, and Procedures." One of those required standards is the Data Loss Prevention (DLP) Operational Standard, outlining the university's DLP implementation. All university-owned computers are required to have the DLP client installed.

How DLP Works

Once the DLP agent has been installed on a computer, the machine will be included in monthly scans, providing insight needed to conduct an inventory of sensitive data, as required by South Carolina state law. If the DLP scan results suggest the presence of sensitive data on your machine, your local system administrator will contact you to determine the most responsible way to store sensitive data. DLP system administrators cannot "read" or access your file contents; they may only view a small selection of information that is believed to concern sensitive data, and only a limited number of authorized individuals have access to the DLP scan results.

Privacy Concerns with DLP

The DLP scan tool searches for ABA bank account and/or routing numbers, credit card numbers, and Social Security Numbers. The university has a right, and a legal responsiblity to protect "university data", as well as your information to help shield the students, faculty, and staff from an unauthorized exposure of information that could negatively impact their lives. As employees or students of the University of South Carolina, the university possesses data about each of us that helps critical functions to operate. For example, university data includes the ABA routing and account numbers for most employees, allowing the proper processing of payroll. That same set of numbers, in the wrong hands, could be devastating to our community.

By helping the university protect sensitive data through the use of DLP technology, you are helping protect information that, if released, could be used to cause financial or reputational harm.

Getting a Head Start on DLP

You can help get a head start on DLP by removing data that is not necessary for normal business operations. In cases where sensitive data is needed, you can work with your local systems administrator for the appropriate procedures to safeguard the information. Any personal data should be moved to a personally-owned computer and then securely deleted from university machines. Remember to empty your Recycle Bin, or use securedelete if on a Mac. Pay close attention to PDF or XLS files, as they have a tendency to be packed full of sensitive information. One quick tip is to search for your own SSN and those of your family. Scans regularly turn up employee tax returns, loan applications, transcripts, etc that the employee may have forgotten about.

UNIVERSITY OF SOUTH CAROLINA
Division of Information Technology

http://security.sc.edu