Data Loss Prevention (DLP) Frequently Asked Questions (FAQ)

End User FAQ

1. What is Data Loss Prevention (DLP)?
   a. DLP is a security technology that is used to discover sensitive data on University owned computers and servers.

2. Why does the University need to deploy DLP technology?
   a. End-users routinely leave old files containing sensitive data on their computers; this technology will identify the files so it can be securely deleted, archived, or the computer secured. This will limit the impact of a data loss in the event a computer is lost/stolen or hacked. In addition, federal and state regulations, and University policy, requires the University to identify sensitive data within information systems and minimize the security and privacy risks associated with the use of that data.

3. This software is an invasion of my privacy. Please remove it immediately!
   a. Per university policy and the data security standards, the software is required to be installed on all university-owned computers. The software should be removed from personally owned devices if installed.

4. Will this software scan my USB thumb drive and external hard drive if they are connected to my computer?
   a. Yes, if it connected to the University owned computer, then they are in scope of the DLP scan.

5. My computer is running slower after you installed the DLP software?
   a. The DLP software is configured to run in the background and throttle down when the computer is in use. DLP software will have negligible impact on the user. The maximum usage is set to 20% CPU utilization when the computer is idle. If you feel this is not the case, please see your local system administrator to determine if there are any application interoperability issues.

6. What kind of data are you scanning for?
   a. Sensitive data, as defined in the Data Security Requirements. Initially, ABA bank routing numbers, credit card, and social security numbers on computers and network file shares. Targeted scans will be conducted of departments that are known to process electronic Personal Health Information.

7. How frequently are you scanning my computer?
   a. UI/ISO will conduct a monthly DLP scan of all University owned computers beginning the first week of each month. The scan can take up to 7 days depending on computer utilization. Most computers will complete the scan on the first day.

8. Will I get in trouble if sensitive data is found on my computer?
   a. No, the scans are meant to identify data and either secure or delete it. If notified of a finding by the security liaison in your department, you must follow their instruction to remediate the finding.
9. What will happen if DLP detects sensitive information on my computer?
   a. The software will flag each finding as an incident in the DLP software. Your organizational unit’s security liaison is required to investigate each incident and bring to resolution. Your security liaison will decide the most appropriate resolution. All incidents are stored in an AES encrypted database within the UTS data center and the data purged after the investigation analysis has been completed.

10. My job requires me to work with sensitive data, will this software prevent me from doing my job?
    a. No, UISO is only using the software to discover sensitive data. At this time, the tool will not be configured to limit the movement of sensitive data throughout the University network. A future goal would be to limit the unauthorized exfiltration of sensitive data outside of the University network.

11. Will the DLP software scan/track my personal email or my web browsing activity?
    a. No, the software is used to discover sensitive data on University owned computer and servers.

Contact
http://security.sc.edu

Revision History

<table>
<thead>
<tr>
<th>Author</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeff Whitson</td>
<td>23-Feb-2015</td>
<td></td>
</tr>
<tr>
<td>Anthony Ryan</td>
<td>04-Mar-2015</td>
<td>Updated document</td>
</tr>
</tbody>
</table>