

**Points of Agreement
Regarding Implementation of Data Loss Prevention Software**

The parties to this agreement, California State University (CSU) and the California State University Employees Union (CSUEU), agree that data breaches are detrimental to all and agree that CSU may proceed with its implementation of the Data Loss Prevention Software, Identity Finder, subject to the following terms of implementation:

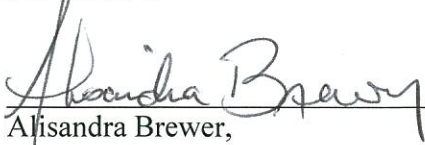
1. The parties acknowledge that CSU is required by law and CSU policy to monitor and protect the security of data used and stored on its systems and acknowledge the importance of working together to ensure the security of the data.
2. The parties recognize the advantages of using a tool such as Identify Finder to assist CSU and its employees in identifying and appropriately securing sensitive data on their workstation computers.
3. Represented employees will receive training regarding the purpose for, set-up, use of, and reporting out from Identity Finder software.
4. Before implementation, each campus will institute an awareness program that gives represented employees a 30-day opportunity to screen their workstations and files to identify and secure any personal information.
5. The campus Identity Finder software console is to be monitored only by the campus Information Security Office.
6. Scans are to be conducted only to identify sensitive data defined as Level 1 or Level 2 data per ICSUAM 8065.S02 Security Data Classification Standards. As currently configured, the software can scan for the following types of sensitive information:

Social Security Numbers
Credit Card Numbers
Password Entries
Bank Account Numbers
Driver's License Numbers
Passport Numbers
Phone Numbers
Personal Addresses
Email Addresses
Australian, Canadian and UK ID Numbers

The campus will not search for phone numbers or personal addresses and will only search for email addresses in conjunction with a previously authorized investigation or to comply with the requirements of Civil Code Section 1798.

7. The campus Information Security Officer may direct employees to scan their own CSU-owned computer workstations periodically to identify sensitive data stored on the hard drive of their computer work stations.
8. The Campus Information Security Office may initiate a scan of employee computers from the campus console periodically to determine whether and how much sensitive data is stored on employee computer workstations.
9. The campus Information Security Office will notify represented employees before the initiation of console-initiated scans on their workstations, unless the workstation is part of an authorized investigation.
10. If sensitive data is found on an employee's CSU-owned computer, the campus Information Security Office will provide the employee with assistance to determine how the employee can protect the information by removing, shredding, redacting, quarantining or encrypting the data.
11. As presently configured, the software scan generates reports of sensitive data found on a user's computer that are viewable by the user but are received by the console as reports of masked data that cannot be viewed at the console.
12. Scans for sensitive data on a user's computer shall not be conducted for the purpose of generating cause to discipline represented employees. However, in the event that an investigation has been previously authorized through existing CSU procedures, reports of Level I or Level II sensitive data on an employee's computer may be used to support disciplinary action pursuant to the applicable Collective Bargaining Agreement or to support criminal prosecution.
13. The Office of the Chancellor shall notify the Unions of the installation of additional modules and/or upgrades to the product that significantly change or enhance the functionality of the software.

For CSUEU:




Alisandra Brewer,
Vice President for Representation
California State University Employees Union

Date

20 February, 2014

For CSU:




William Perry,
Chief Information Systems Officer
Office of the Chancellor
California State University

Date

3-3-2014


Rich McGee,
Bargaining Chair
California State University Employees Union

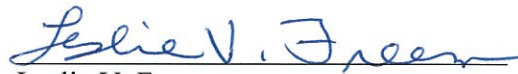
2/20/14
Date


Ed Hudson,
Information Security Director
Office of the Chancellor
California State University

3/3/14
Date


Tessy Reese,
Bargaining Unit Chair Unit 2
California State University Employees Union

2/20/14
Date


Leslie V. Freeman,
Manager, Labor Relations
Office of the Chancellor
California State University

3/3/14
Date


John Orr
Bargaining Unit Chair Unit 7
California State University Employees Union

2/20/14
Date


Susan Smith
Bargaining Unit Chair Unit 9
California State University Employees Union

2/20/14
Date