Data Loss Prevention (DLP)

Introduction: Data Loss Prevention

The College of Engineering uses Broadcom’s Symantec DLP suite in order to comply with the OSU Information Security Control Requirements (ISCR). These requirements exist to safeguard you and the University against legal, regulatory, monetary and reputational liabilities related to the improper storage of restricted data such as social security numbers, bank account and credit card information.

What is Data Loss Prevention?

Data Loss Prevention (DLP) refers to our efforts to classify, identify and manage restricted data on College of Engineering computer systems. The goal of DLP is to mitigate risks associated with storage of – and access to – restricted institutional data.

Why is Data Loss Prevention important?

As an organization, OSU is bound to several legal, regulatory and compliance obligations due to the nature of the data we handle. As a result, the College of Engineering is required to understand the type and nature of data stored on departmental computers.

What is considered restricted data?

Restricted data is data that is bound to certain legal, regulatory and contractual requirements as described in the OSU Information Security Standard (ISS) and Information Security Control Requirements (ISCR) policies. Restricted data includes (but is not limited to) Social Security Numbers, FERPA/HIPAA data, Payment Card Industry information, or other data that is intended for limited use and availability.

How do OSU’s Data Loss Prevention policies affect me?

The College of Engineering has deployed Broadcom’s Symantec DLP suite to discover and evaluate institutional data on college-managed systems. Symantec will be used to scan systems managed by ETS in order to identify restricted data and to ensure that it is being properly stored and accessed.

When did the College of Engineering implement the Spirion Data Security Software?

ETS has been actively deploying Symantec DLP since Fall Quarter of 2020.

Who can I speak with regarding concerns I have with this phase of OSU’s DLP implementation?

Questions, comments and concerns can be addressed to the Engineering Technology Staff via the ETS Service Desk Portal or by email to etshelp@osu.edu. We will do our best to ensure that your question, comment or concern is addressed in a timely manner.

Your Responsibilities

What are my responsibilities?

As a College of Engineering faculty, staff, student or affiliate you have a responsibility to ensure that data you handle is stored and accessed in accordance with Ohio State University IT Security Standards Policy: https://ocio.osu.edu/policy/standards/security. If you are aware of – or become aware of – restricted data residing on systems you use, it is your responsibility to take the appropriate measures to ensure that the handling and access of your data is in compliance with university policy.

Deployment, Discovery and Remediation
Spirion Identity Finder works by scanning computers for restricted data. In the past, the software alerted ETS staff to the presence of restricted data that appeared to be improperly stored. When that occurred, ETS worked with departmental IT staff to delete the data or move it to systems compliant with the OSU ISCR.

ETS is currently in the process of deploying an updated version of Spirion Identity Finder to all College of Engineering computer systems. As part of this upgrade, an interactive feature of the software is being implemented. The interactive feature will alert the user (You!) to the presence of restricted data, and give you the option to shred (ie permanently delete) the data.

**How it works:**

Broadcom’s Symantec DLP will scan your computer as per the [College of Engineering DLP Monthly Scan Schedule](http://go.osu.edu/ets).

The process is intended to be invisible to the user. When restricted data is discovered, ETS Staff will create remediation requests via the [ETS Service Web Portal](http://go.osu.edu/ets).

**Broadcom’s Symantec DLP (General Information)**

**About Symantec DLP**

Symantec DLP suite is software capable of scanning file systems in order to find sensitive data such as:

- Social Security Numbers
- Credit Card Numbers
- Bank Account Numbers
- Driver’s License Numbers
- Passport Numbers
- Additional Data Types

Symantec DLP will...

- Scan all files
- Generate reports which can be viewed by DLP administrators

Symantec DLP will NOT...

- Copy files
- Alter data

**Requesting a filesystem scan**

If you would like to request a file system scan outside of the College of Engineering DLP Monthly Scan Schedule, please contact Engineering Technology Services via the [ETS Service Web Portal](http://go.osu.edu/ets) or via email to etshelp@osu.edu.

If you need assistance, please contact Engineering Technology Services:

**Phone:** (614) 688-2828

**Email:** etshelp@osu.edu

**Service web portal:** [http://go.osu.edu/ets](http://go.osu.edu/ets)

**Service Desk Location:** 1012 Smith Lab

**Business Hours:** M-F 7:00 A.M.-5:00 P.M.