DATA LOSS PREVENTION AND DATA CLASSIFICATION

DATA LOSS PREVENTION
INFORMATION SESSION

January 2021
University Information Security Office and Data Loss Prevention Working Group
Agenda

- Project Team
- Background
- User Focused Security
- Information Classification
- Data Handling
- Deployment & Next Steps
Project Team

Working Group:

- Rita Vazquez, Registration and Records
- Danielle Hanson, HR
- Rebecca Gomez, Finance
- Cory O’Brien, Treasury
- Karen Cornelius, Risk
- Ron Price, AVP Informatics & Clinical Research
- Jessica Shore, Clinical Research
- Josie Corral, Clinical Research
- Jim Pardonek, Chief Information Security Officer
What is Data and Its Risks?

- Data is one of the University's most valuable assets.
- Because staff need to handle Sensitive and Protected Data, it is necessary to educate employees on how to properly secure data.
- Universities have an increasing dependency on information in the form of computer data for their day-to-day operations.
- The risk of data being misused or accidentally/deliberately modified or damaged increases.
- Damage to Loyola’s reputation.
Background Information

Who is Affected?
- Anyone who creates or handles sensitive or Protected data.
- Sensitive and Protected data exists throughout the University.

What to Know?
- How to recognize Sensitive and Protected data.
- What precautions are needed to take when “handling” them.
- Certain types of data must be specially handled so that the Loyola can maintain its operations while fulfilling its legal or moral obligations.
Challenges – Implementing Data Classification and Protection at Loyola

- Management/ Information Security may not have knowledge of:
  - What data exists;
  - Where it is;
  - Who owns it
  - What level of protection is required; and
  - How to protect it

Solution – Data Labeling

- Protecting information requires data labeling tools that are safe and easy to use to protect the:
  - **Confidentiality** of data, where sensitivity warrants
  - **Integrity** of data, to ensure its completeness and accuracy
  - **Availability** of data, so that it is accessible when required.
How Data Loss Prevention Applies Across the Institution

Benefits of Protecting Data

- Protection of Patient Research Data
  - Ron Price, AVP, Informatics, ITS
- Keeping Employee Data Safe
  - Danielle Hanson, AVP, HR
- Why Payroll is Important
  - Becky Gomez, AVP, Financial Systems & Payroll
- Student Data Protection
  - Rita Vasquez, Registrar and Director, Reg and Rec

Data owners are people with the best knowledge of how to identify and classify the data they own.
User-Focused Security

People
- Data Owners
- Data Users

Policy
- Data Classification Policy
- Cloud Computing Policy
- Third-party Data Handling Requirements

Technology
- Data Classification System
- Data Loss Prevention Solution

DATA
Why Do We Need Data Loss Prevention?

- Assist departments with understanding how and where they are storing, accessing, and sharing data with others.
- Protect against data loss (data accidentally leaving the University).
- Protect University data (classify data and create safeguards for how data is shared).
- Remind users how to safely share data outside of the University.
Data Loss Prevention (DLP) helps manage content being shared outside the University.

- Notifies a user when they may be sharing sensitive or protected information outside of Loyola.
- Helps classify and protect documents and emails by applying labels to documents.
- Labels remain with the document as a sensitivity property.
- Labels are based on Loyola’s Data Classification policy.

Data Loss Prevention Business Benefits.

- Helps each department identify what documents/data they use.
- Helps to better understand what documents/data are shared with others outside of Loyola vs shared internally.
- Prevents the accidental release of Protected and Sensitive information.
Public Data

- Information which may or must be open to the general public.
- It is defined as information with no existing local, national, or international legal restrictions on access.
- Examples: reports containing generalized information (e.g. summary reports, enrollment reports, degrees conferred reports), or any report that contains only directory information.
Sensitive Data

- Information whose access must be guarded due to proprietary, ethical, or privacy considerations.
- This classification applies even though there may not be a civil statute requiring this protection.
- Examples: LOCUS ID, Lawson ID, electronic signatures.
Protected Data

- Information protected because of protective statutes, policies, or regulations.
- Data for which a data owner exercised their right to restrict access.
- Example: FERPA, PII, HIPAA, credit card data, U.S. financial data, etc.

Public

Sensitive

Protected
Proper Data Handling

• It is important to understand how to classify data based on the data type and different levels of precautions for handling during its life cycle.

  • Creation and Access
  • Disclosure and Sharing
  • Storage
  • Copying and Transmitting
  • Printing
Demonstration
Demonstration
<table>
<thead>
<tr>
<th>Name</th>
<th>Date modified</th>
<th>Type</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Microsoft Word Document.docx</td>
<td></td>
<td></td>
<td>13 KB</td>
</tr>
<tr>
<td>New Microsoft Excel Worksheet.xlsx</td>
<td></td>
<td></td>
<td>7 KB</td>
</tr>
</tbody>
</table>
Demonstration

Classify and protect - Azure Information Protection

Multiple files selected

<table>
<thead>
<tr>
<th>Not set</th>
<th>Loyola Public</th>
<th>Loyola Sensitive</th>
<th>Loyola Protected</th>
</tr>
</thead>
</table>

- Delete Label

- Protect with custom permissions

- Remove Custom Permissions

[Apply] [Close]
Demonstration
Demonstration
Demonstration

Policy tip: Your email message conflicts with a policy in your organization. Hide details

This recipient isn't authorized to receive this type of information. Remove recipient

View details about the information that appears sensitive. Learn more

This message appears to contain the following sensitive information:

- LUC - U.S. Social Security Number (SSN)

If you don't think this information is sensitive, please click Report.

Report

To

Cc

SSN alert test

SSN: 535-43-4626
Demonstration

Override (Web Access Client)

Override (Outlook Client)
Notification: SSN alert test

You are receiving this notification because content shared by you may conflict with Loyola University Chicago's data security policies, based on the following issues:

- Message is sent to people outside your organization.
- Message contains the following sensitive information: LUC - U.S. Social Security Number (SSN)
- Following Senders violate organizational policy: 'a56394c9-a371-4895-9880-e731b7e7e7ba'.

Please refer to the Electronic Security of Loyola Protected & Loyola Sensitive Data Policy for more information.

Message is attached.

Loyola Protected or Sensitive information should only be shared with people outside the University when it’s absolutely necessary, and should always be sent securely via Loyola Secure Transfer.

Questions regarding this notification or the data security policies may be directed to the University Information Security Office (UISO) via the ITS Service Desk at ITSServiceDesk@luc.edu or 773-508-4487.
What happens if I get a false positive?

- **False Positives Reporting Steps**
  - No Data Loss Prevention system is perfect.
  - If you get a policy tip for a DLP rule.
  - You have the option to "report" your content as a false positive.
  - Clicking “Report” creates a log entry for reporting purposes only.
  - False Positives requiring an explanation should be reported to the ITS Service Desk.
  - You can then allow and reclassify and share or send the file.
Can I override a false positive?

- **Override Feature**
  - Some data types allow the user to override and reclassify an email or document.
  - Data types that allow for an override will display an override button withing the policy tip.
  - You have the option to “override” your content as a false positive.
  - Clicking “Override” creates a text box for an explanation of the reclassification.
  - Overrides are sent to the Data Owner for later review.
  - You can then allow and reclassify and share or send the file.
I really need to send this file/email, what do I do?

• **Loyola Secure Transfer**
  • Send, Receive and Share Files of any file size in and out
  • Send Unlimited Sized Files to anyone using a simple Webmail-like Interface
  • Receive Unlimited Sized Files from anywhere
  • Request Files with a simple link for the receiver to use when responding to the request.
  • Video instructions can be found at: [https://www.luc.edu/its/uiso/resources/loyolasecuretransfer/](https://www.luc.edu/its/uiso/resources/loyolasecuretransfer/)
Where are we today?

- **Initial Deployment (November 2020):**
  - Manual labeling of Microsoft documents when saving.
  - Providing a justification for downgrading a document's classification (once labeled).
  - Notifications when sharing content that should not be shared externally.

- **Sensitive Data Types:**
  - Provide feedback/requests for additional configuration.
  - Provide suggestions to Service Desk or project team.
Next Steps

• **Deployment (March-April 2021):**
  • Automatic labeling of documents, based on data content.
  • Blocking data that should not be shared externally.
  • Providing a justification for sharing protected data with external users based on the type of data. Some data types cannot be overridden.

• **Effects on email forwarding rules:**
  • All Protected data will be blocked and will not forward.
  • The warning notice email message will be sent to both the LUC email and the forwarded email.
  • Users will need to use their LUC email to view protected data.
  • Recommended use of Loyola Secure Transfer if transmitting protected data is necessary.
Conclusion

• Even with a well-defined classification and handling policy and document management software, it is still PEOPLE who:
  • Identify and classify information
  • Handle the data
  • Operate the technology
• Users should always be aware of the importance of data and thus the classification and handling requirements.
Questions?

Thank you for attending!