Electronic Security Protected-Sensitive Data Policy

Policy Title:
Electronic Security Protected-Sensitive Data Policy

Responsible Executive(s):
Jim Pardonek, Director and Chief Information Security Officer

Responsible Office(s):
University Information Security Office (UISO)

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy covers any data that has been classified as either Loyola Protected data or as Loyola Sensitive data and is stored or transmitted electronically (covered electronic documents). The purpose of this policy is to provide security practices for employees, student workers, consultants or agents of Loyola University Chicago and any parties who are contractually bound to handle data produced by Loyola, who produce or have access to covered electronic documents.

II. Definitions

Covered electronic documents: Any data that is classified as either Loyola Protected data or as Loyola Sensitive data and is stored electronically.

LSA: Loyola Secure Access, the Loyola branded version of virtual private network (VPN).

III. Policy

Additional precautions shall be used by any departments or individuals who have access to covered electronic documents. These additional precautions include:

Encryption

ITS provides and requires full disk encryption technology to protect all University managed computers identified during the compliance review as containing covered electronic documents.

Users who know that their computer will store covered electronic documents should, in accordance with Loyola's Encryption Policy, contact the ITS Service Desk at ITSServiceDesk@luc.edu to request an installation of the full disk encryption software. ITS will provide training in using encryption software to the users of these systems.

Storage of Covered Electronic Documents

Users shall store covered electronic documents on approved network storage instead of local hard drives or any form of removable media. In cases of a granted exception, the computer must run a full disk encryption product provided by ITS.

Loyola Protected data must never be stored on unapproved media. Loyola Sensitive data can be stored for remote access upon permission of the department owning the data. The acceptable storage options for Loyola Sensitive data are listed below in order of preference:

- Networked storage
- University owned laptop running approved encryption software
- Portable drive using approved encryption software
- CD/DVD/Disk saved as an encrypted file using approved encryption software

Passwords

The user shall protect any resources that house covered electronic documents with a password. This password must meet or exceed the current ITS password standards described in Password Standards.

Limited access – At Loyola

All areas that contain computers storing covered electronic documents should only be accessible to employees, student workers, consultants, or agents of Loyola University Chicago that have a business need for access. Individuals not affiliated with Loyola University Chicago must not have unsupervised access. Department heads or their designee will work with Campus Safety to control access through either a physical key or via a badge reader. Areas that cannot be locked cannot be used to house computers that store covered documents. Department heads or their designee will identify individuals who have a need to access these areas to perform their job function and will communicate the names of these individuals and their required access to Campus Safety. When leaving their desk in an area containing computers with access to covered documents, individuals shall either lock their computer or log off. Off campus access requires the use of the University's Virtual Private Network

(VPN) branded as LSA.

Limited access – Outside of Loyola

Non-Loyola spaces used by contracted 3rd parties should only be accessible by individuals the contractor has approved to access covered electronic documents. All areas that contain computers storing covered documents must not provide unsupervised access to the public. Areas that cannot be locked cannot be used to house computers that store covered documents. When leaving their desk in an area containing computers with access to covered documents, individuals shall either lock their computer or log off.

Data Loss Prevention

The University has employed technologies designed to protect against the intentional or inadvertent transmission or sharing of covered electronic documents. These technologies protect the following services:

- Email
- OneDrive
- SharePoint
- Others may be added at time of deployment

If an individual attempts to send or share any covered electronic documents using these services, the action will be logged and they will receive a notification stating why the content may violate University policy.

Any of the following actions may follow:

- Action has been prevented
- Content will be blocked
- User will be provided an opportunity to justify the action
- Content will be encrypted

Training

ITS and HR will make training materials available to all staff with access to covered electronic documents which will cover all issues raised in this policy in greater detail.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Jim Pardonek, Director and Chief Information Security Officer	Enforcing the Policy at the University by setting the necessary requirements.

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- Data Classification Policy
- Encryption Policy
- Password Standard

Approval Authority:	ITESC	**Approval Date:**	March 4th, 2008
Review Authority:	Jim Pardonek	**Review Date:**	March 7th, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu