Physical Security of Loyola Protected-Sensitive Data Policy

Policy Title:
Physical Security of Loyola 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 classified as either Loyola Protected data or as Loyola Sensitive data and stored on paper (covered paper documents).

The purpose of this policy is to provide physical 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 paper documents.

II. Definitions

Not applicable.

III. Policy

For departments within Loyola, department heads will be responsible for implementing additional precautions to be used by any individuals in their department who have access to covered paper documents. Contracted 3rd parties will be responsible for implementing additional precautions to be used by their employees. These additional precautions include:

Limited access – At Loyola

All areas that contain covered paper documents should not be accessible to all employees, student workers, consultants, agents, or visitors of Loyola University Chicago. All areas that contain covered paper documents must not provide unsupervised access to the public. Department heads or their designee will work with Campus Safety to control access to areas containing covered paper documents via either

a physical key or a badge reader. Areas that cannot be locked cannot be used to store covered paper 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 covered paper documents, individuals shall, to the best of their ability, properly put away and secure covered paper documents.

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 paper documents. All areas that contain covered paper documents must not provide unsupervised access to the public. Areas that cannot be locked cannot be used to store covered paper documents. When leaving their desk in an area containing covered paper documents, individuals shall, to the best of their ability, properly put away and secure covered paper documents.

Cleaning staff

For departments which contain covered paper documents, the department head or their designee will determine if it is practical to request that the cleaning staff perform their duties during normal business hours, while the area is staffed. If none of the department employees are present, the cleaning staff will not clean that area at that time. If a department has covered paper documents but receives cleaning services after hours, then employees shall, to the best of their ability, properly put away and secure covered paper documents before ending their workday. Cleaning staff will not have master keys for any areas which they clean during normal business hours.

Printers and Fax Machines

Department heads or their designee will work with ITS and Facilities to ensure that all printers and fax machines that output covered paper documents will be in a limited access area. In areas where this is not possible, employees, to the best of their ability, will not leave printed or faxed covered paper documents unattended for long periods of time.

Designated shredding containers

For departments that handle covered paper documents, the department head or their designee will work with Purchasing to ensure that the department has access to a secured repository in which they can deposit covered paper documents to be shredded.

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

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