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 82j00u0T-7 (t) csy-6Jvt conu0T-.9 (lila-2 (v-2 (vif.14 Td-)9(10 (n) a-2 (v

(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 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