UNIVERSITY
of ARKANSAS
AT PINE BLUFF
1873

DATA LOSS PREVENTION (DLP) POLICY

INTRODUCTION

This policy is a guide in identifying and gaining an understanding of the components of the University of Arkansas at Pine Bluff (UAPB) that make up its information security system and thereby enable UAPB to manage risk to systems, assets, data, and capabilities.

POLICY

Data Loss Prevention (DLP) is a set of technologies and business policies to make sure end-users do not send sensitive or confidential data outside the organization without proper authorization. DLP enforces remediation with alerts, encryption, and other protective actions to prevent end users from accidentally or maliciously sharing data that could put the organization at risk. Sensitive information might include financial records, customer data, credit card data, or other protected information. The most common method that this data is leaked is via email.

POLICY INFORMATION

Beginning June 1, 2020, all email and one drive that contains sensitive information will be automatically blocked. The sender will receive an Outlook message when an email is sent that contains sensitive information. Faculty and staff can still manually encrypt any email.

BEST PRACTICES

- Do not forward email you receive that contains sensitive information. If it is required to do so, redact the sensitive information before replying.
- Seek alternate means of transmitting the sensitive data. (secure web applications, etc.)

Continuous improvement. The content of this document subject to regular review based on input from UAPB Technical Services staff and the campus community. Recommendations for development should be submitted to the Director of Technical Services. Awaiting approval.