SOUTHEAST MISSOURI STATE UNIVERSITY · 1873	BUSINESS POLICY AND PROCEDURE MANUAL	Date Issued: 09/18	Revision Date: 05/26	Page: 1 of 1
				Classification Code: 10-11
		Section: INFORMATION TECHNOLOGY		
		Subject: DATA SECURITY		

GENERAL STATEMENT OF POLICY:
This policy reflects the University's commitment to use appropriate integrity controls to protect the confidentiality and integrity of sensitive University data at rest or while transmitted over electronic communications networks.

POLICY:
Data considered sensitive or protected by Southeast Missouri State University is personally identifiable information (PII) such as Social Security or Driver's License numbers, email addresses, home addresses, birthdate, health information, financial information, employment records, etc. Additionally, University financial, Human Resources or legal information not cleared for the public is also considered sensitive/protected data.

Further, any system or application that provides access to university data should implement role-based access procedures or restrictions to manage appropriate access based on work requirements/job function.

1. Encryption should be used to protect the confidentiality and integrity of university data at rest or transmitted over a communications network including email or mobile devices. All encryption methods used to protect the confidentiality and integrity of university data at rest or transmitted over an electronic communications network must be approved by the University Information Security Officer.

2. The use of E-Mail to transmit sensitive business information is strongly discouraged, except when Information Technology approved controls are used to ensure the confidentiality and integrity of the data.

3. All University owned and managed mobile equipment (phones, laptops, tablets, etc.) must be encrypted.

4. Any removable storage devices (external hard drives, USB thumb drives, etc.) used to store or move sensitive university data must be encrypted.

5. Web applications, Software-as-a-Service (SaaS) or any other 3rd party services must use the appropriate protocols to ensure data is secured.

The Assistant Vice President for Information Technology is responsible for maintaining operating procedures associated with this policy.