



## POLICY STATEMENT 130 INFORMATION TECHNOLOGY APPLICATION SECURITY

### POLICY DIGEST

Monitoring Unit: Office of Information Security

Initially Issued: April 20, 2023

Last Revised: April 20, 2023

### I. PURPOSE

As an institution of higher education, the Louisiana State University at Eunice Campus (“University” or “LSU Eunice”) is charged with maintaining systems and data for administrative, academic, and research purposes. Applications that support University’s business are critical and must be managed with a formalized Application Security Policy.

The purpose of this policy is to define the required processes and activities pertaining to application security.

### II. DEFINITIONS

**Application.** A system for collecting, saving, processing, and presenting data by means of a computer. An application developed internally by an organization will be referred as custom application.

**Asset.** A resource, process, product, information infrastructure, etc. whose loss or compromise could intangibly affect its integrity, availability, or confidentiality, or it could have a tangible dollar value. The loss or compromise of an asset could also affect an entity’s ability to continue business. Examples of assets including, but are not limited to, equipment, software, algorithms, and data.

**Data.** Any information residing on the University IT Infrastructure or held on any other IT Infrastructure on behalf of the University. This data includes files, documents, messages in any format, including e-mail messages and posts made on any Social Media site maintained by/for the University or its units. All data created and/or maintained by a User is also subject to this Policy, even if the data is created and/or stored on the User’s own personal computer, smartphone, or other personal device.

**Information Technology Asset.** An IT Asset is a subset of Asset and specifically refers to hardware (laptops, desktops, servers/virtual servers, external storage devices, mobile devices, etc.) utilized to store, process, access, and/or handle Data.

**Software as a Service (SaaS).** The capability provided to a consumer to access or use a provider’s application running in a cloud infrastructure. SaaS can also be referred as Cloud Application.

42 **III. POLICY STATEMENT**

43 A. Secure Application Development

44 1. LSU Eunice shall ensure the secure software development practices are followed  
45 during the entire software development lifecycle and implement controls  
46 appropriately, for all applications that are developed internally, i.e., within LSU  
47 Eunice, or through a partnership with a third-party vendor.

48 2. LSU Eunice must define and incorporate appropriate security architecture for all  
49 custom applications developed internally.

50 B. Application Security Review

51 1. LSU Eunice shall develop processes and procedures to test and verify the security  
52 posture of all custom applications prior to the move of the application to production  
53 environment.

54 2. LSU Eunice shall develop processes and procedures to assess security posture of  
55 all custom applications throughout the life of the application.

56 C. Cloud Application

57 1. LSU Eunice shall develop processes and procedures to evaluate security posture of  
58 all cloud applications utilized by the institution.

59 **IV. STANDARDS**

60 A. The Secure Application Development standards are outlined in LSU Eunice-ST-130-1

61 B. The Application Security Review standards are outlined in Standard LSU Eunice-ST-  
62 130-2.

63 C. The Cloud Application standards are outlined in Standard LSU Eunice-ST-130-3.

64 **V. REVISION HISTORY**

Version	Date	Change Description	Edited By
0.1	11/21/2022	Initial Draft	Office of Information Technology

65