



POLICY STATEMENT 123 STANDARD 2 EMPLOYEE LIFECYCLE

POLICY DIGEST

Monitoring Unit: Office of Information Technology

Initially Issued: December 12, 2022

Last Revised: none

I. PURPOSE

As an institution of higher education, Louisiana State University at Eunice (“University” or “LSU Eunice”) is charged with maintaining systems and data for administrative and academic purposes. These assets are critical to the mission of the University, and the acceptable use of these systems and data sets must be managed with a formalized Information Security Program.

A major element of protecting the University’s Information Technology (IT) assets is ensuring personnel are aware of security responsibilities at every phase of employment.

The purpose of this standard is to describe security procedures that should be followed at all stages of the employee lifecycle at the University.

II. DEFINITIONS

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 LSU Eunice’s ability to continue business.

Personnel. All users that are hired or otherwise engaged by the University to perform a particular task, job, and/or duty. This includes full-time and part-time employees, including student employees and contract employees.

User. Any individual or entity that utilizes an asset. A user can be an individual, application, information system, network, etc.

III. STANDARDS

A. Recruiting

1. LSU Eunice must conduct background checks on all personnel who have been selected for employment.
2. LSU Eunice must identify and document all positions that require extended background check including credit checks.
3. LSU Eunice must conduct extended background checks for employees that are changing positions to the identified positions that require it.

- 40 B. Onboarding
- 41 1. LSU Eunice must identify and provide computing resources and the associated
- 42 access to said resources to support the academic, educational, and any research
- 43 initiatives of the University.
- 44 a. All access must be related to the position an employee has been hired for.
- 45 b. Any request for access must be initiated by the supervisor or departmental
- 46 contact.
- 47 c. All efforts must be made to provide relevant access through an automated
- 48 fashion based on position and responsibilities, where applicable.
- 49 2. LSU Eunice must implement processes and procedures to attain acknowledgement
- 50 from users of their responsibilities as they pertain to the use of technology and
- 51 access.

52 C. Termination and/or change of status

- 53 1. Human Resource Management (HRM) must notify the OIT team if account/system
- 54 access must be removed and/or modified in any manner that deviates from
- 55 established automated termination procedures.
- 56 2. Supervisors must recover all IT assets from a terminated employee prior to or on the
- 57 last day of affiliation with the department and/or University. This may include, but is
- 58 not limited to, laptops, tablets, mobile devices, desktops, access identification cards,
- 59 access keys, and any other University property.
- 60 3. When an employee's position changes, supervisors of old and new position must
- 61 ensure that all relevant access has been removed and/or added as applicable for the
- 62 employee.
- 63 4. Individuals responsible for engaging contracted individuals/entity must follow
- 64 established processes and procedures to terminate granted access when the work
- 65 effort has been completed.
- 66 5. OIT must conduct annual audits of all guest accounts and access to determine guest
- 67 status.

68 **IV. REVISION HISTORY**

Version	Date	Change Description	Edited By
0.1	04/20/2022	Initial Draft	OIT

69