POLICY STATEMENT 128
IDENTITY AND ACCESS MANAGEMENT

Monitoring Unit: Information Technology Services
Initially Issued: July 21, 2023

PURPOSE

As an institution of higher education, the Louisiana State University A&M Baton Rouge Campus (“University” or “LSUAM”) is charged with maintaining systems and data for administrative, academic, and research purposes. These assets are critical to the mission of the University, and risks assessments performed around these systems and data sets must be managed with a formalized Identity and Access Management Policy.

The purpose of this policy is to define the required processes involved in the management of identities and their associated access to information assets.

DEFINITIONS

Account – Account(s) associated with an identity utilized to access IT Assets. Typically comprised of a username and password.

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 University 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.

Identity – An attribute or set of attributes that uniquely describe a subject within a given context.

IT Asset – For the purpose of these policies, IT Asset is a subset of Asset and specifically refers to hardware that have compute and storage capabilities (e.g., laptops, desktops, servers/virtual servers, mobile devices, etc.) and is utilized to store, process, access, and/or handle Data.

Principle of Least Privilege – The principle requires that a user/system is only granted the least level of access for the least amount of time necessary to perform their job and/or duties.

Single Sign On (SSO) – An authentication and session management solution allowing a user to leverage a single account and authentication process to access multiple applications.

POLICY STATEMENT

A. Identity Management
   1. LSUAM shall define minimum attributes that constitute an identity record.
   2. LSUAM shall define processes and procedures to maintain an identity lifecycle.
   3. LSUAM shall establish processes and procedures that direct the assignment, storage, and maintenance of identities.

B. Account Management
   1. LSUAM shall implement categories of account types that may be available at the University.
   2. LSUAM shall define processes and procedures for account lifecycle management (e.g., creation, suspension, retention schedule, deletion, etc.).

C. Authentication Management
   1. LSUAM shall implement enterprise authentication mechanisms to be used for access to information resources.
   2. LSUAM shall implement password requirements for all accounts.
   3. LSUAM shall implement and make available security controls to enhance authentication security where applicable.
   4. LSUAM shall leverage enterprise Single Sign On (SSO) technologies to standardize authentication experience.

D. Authorization Management
   1. LSUAM shall document and define all enterprise authorization mechanisms used to access IT assets.
   2. LSUAM shall implement principle of least privilege where applicable.
   3. LSUAM shall implement processes and procedures for access and authorization for privileged accounts.
   4. LSUAM shall implement processes and procedures for audits related to access reviews.

STANDARDS

A. The Identity Management standards are outlined in Standard PS-128-ST-1.

B. The Account Management standards are outlined in Standard PS-128-ST-2.

C. The Authentication Management standards are outlined in Standard PS-128-ST-3.

D. The Authorization Management standards are outlined in Standard PS-128-ST-4.

EXCEPTIONS AND NON-COMPLIANCE

- Please refer PS-120-ST-4 for additional information related to exceptions.
- Please refer PS-120 for additional information related to Policies and Standards non-compliance.

REVISION HISTORY

Version	Date	Change Description	Edited By
0.1	7/21/2023	Initial Draft	Information Technology Services