PRIVILEGED IDENTITY MANAGEMENT POLICY

Purpose

The purpose of this policy is to define required access control measures to all RSBPL systems and applications to protect the privacy, security, and confidentiality of RSBPL information assets and systems, especially highly sensitive systems.

Scope

This policy is applicable to those responsible for the management of user accounts or access to shared information or network devices. Such information can be held within a database, application or shared file space. This policy covers departmental accounts as well as those managed centrally.

Definitions

Access- The ability to use, modify or manipulate an information resource or to gain entry to a physical area or location. Access Control- The process of granting or denying specific requests for obtaining and using information. The purpose of access controls is to prevent unauthorized access to IT systems.

Availability- Protection of IT systems and data to ensure timely and reliable access to and use of information to authorized users. Confidentiality- Protection of sensitive information so that it is not disclosed to unauthorized individuals, entities or processes. Principle of Least Privilege- Access privileges for any user should be limited to resources absolutely essential for completion of assigned duties or functions, and nothing more. Principle of Separation of Duties- Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse, or other harm

Identification

Identification is the process of assigning an identifier to every individual or system to enable decisions about the levels of access that should be given. Identifiers must contain the following:

Uniqueness- Each identifier (e.g. user ID) is unique; that is, each identifier is associated with a single person or other entity

One Identifier per Individual- An individual may have no more than one Unique identification number

Authentication

The authentication process determines whether someone or something is, in fact, who or what it is declared to be. Authentication validates the identity of the person. Authentication methods involve presenting both a public identifier (such as a user name or identification number) and private authentication information, such as a Personal Identification Number (PIN) or password. All systems and applications must use encrypted authentication mechanisms and abide by the following:

Authentication credentials will not be coded into programs or queries unless they are encrypted, and only when no other reasonable option exits.

Unique initial passwords must be provided through a secure and confidential manner and initial passwords must be changed upon first logon

Passwords must not be stored in clear text or in any easily reversible form.
Vendor-supplied default and/or blank passwords shall be immediately identified and reset upon installation of the affected application, device, or operating system.
To ensure that passwords are of adequate strength, passwords for users, systems, applications, and devices must meet, to the degree technically feasible, the following Information Security requirements:

Password Requirements	
Password Expiration	Every 90 days
Minimum Length	8 characters
Password Complexity	Enabled
Password History	Last 4 passwords
Account Lockout	After 5 unsuccessful consecutive logon attempts
Lock-Out Duration	30 minutes
Renewed Log In	After 30 minutes of inactivity or by a system administrator
Screensaver	Idle after 10 minutes, password protected