



INFORMATION SERVICES
User ID and Password Policy
POLICY Number: C-001

1 March 2013

1. **AUTHORITY:** Director of State Civil Service as contained in La R.S. 36:54
2. **REFERENCES:** Office of Information Technology Technical Standard/Procedure IT STD 1-01 (Security: Authentication/Passwords)
3. **PURPOSE:** To establish a method of protecting information technology systems from unauthorized access, modification and destruction.
4. **APPLICABILITY:** This policy shall apply to all employees of State Civil Service.
5. **DEFINITIONS:**
 - A. **User ID** – a unique identifier that allows the computer system to recognize an individual as an authorized user. User ID's are used as a component of security to grant the appropriate level of access to each employee.
 - B. **Authentication** - the verification of the identity of a person or process. A password is a secret series of characters that, by association with a user-ID, allows access to information, systems, applications, or networks.
6. **POLICY:** It is the Director's policy that State Civil Service shall require procedures for authorizing, revoking, and resetting User ID's and passwords to include a method by which to verify the identity of the person requesting the action. Requirements shall also be in place for a reasonable number of unsuccessful login attempts allowed prior to revocation of password, maximum validity periods for passwords, and password re-use limitations.

7. PROCEDURES:**A. USER ID – ESTABLISHMENT AND REVOCATION**

1. It will be the responsibility of each Division Administrator to request the establishment or revocation of User ID's for each employee in his or her Division. This request shall be prepared through memorandum or email.
2. MIS must receive written notification from the Division Administrator approving authorization or revocation of a User ID or password at least 3 business days prior to the requested effective date whenever possible.
3. The MIS Division will be responsible for the management of USER ID's and passwords.

B. PASSWORD REQUIREMENTS

1. Passwords shall be kept confidential.
2. Minimum password length and format shall adhere to the set standards of each system/application.
3. Passwords shall not be kept on paper or stored in plain text format.
4. All passwords shall be changed whenever it is determined that a system's security may have been compromised.
5. Passwords shall be changed on a regular basis, not greater than 30 days.
6. Passwords shall not be included in a macro or function key to automate login processes.
7. Temporary or "reset" passwords shall be changed upon first use.
8. After three successive unsuccessful attempts at login, the user id shall be marked inactive and require a reset before additional login attempts are possible.
9. Intrusion detection software will be used where applicable to deter unauthorized attempts at guessing passwords.

8. **EXCEPTIONS:** The Director of State Civil Service may grant an exception to any provision of this policy, provided such exception shall not be in conflict with Civil Service Rules and Regulations.

s/Shannon S. Templet
Director