



User Password Policy

Subject User Passwords	Approval Signature <i>Julie Ruthven</i>
Who this Policy Applies to Employees and Customers of SOS	Approval Date 08/06/2008
Number 20.11.3	Scheduled Review Date 08/05/2009

Purpose

To establish a standard for changing, unlocking or resetting user passwords to help minimize the risks of social engineering, fraud, and misuse. To address information technology security concerns raised during password change requests by all Oregon Secretary of State (Secretary) employees, contractors and external users who use the Secretary's information processing systems.

The scope of this policy is to address the use of user passwords. User passwords are owned by an individual. All accounts with the agency's naming convention of user passwords are covered by this policy. External users of applications via Oracle Identity Manager (OIM) are also in scope of this policy.

The scope of this policy does not include user accounts with Department of Administrative Services (DAS) application. These include but are not limited to: ePay, SPA and mainframe.

The following definitions of accounts and passwords are out of the scope of this policy:

Account	Definition
Batch Processing Account	An account and password known by authorized agency employees to log into applications to perform business functions.
Development Database Account	Accounts in the development environment that are used for the development and testing of an application.
Look Accounts	A password known by agency employees to log into applications to grant limited access to the application and test application functionality.

- Focused on Security. Dedicated to Success. -



User Password Policy

Production Database Account	An account and password known by authorized agency employees to log into applications to perform business functions.
QA Database Account	Accounts in the QA environment that are used for testing an application.
System Password	An un-spaced sequence of characters that provides access to infrastructure components such as servers, network appliances, and databases. System passwords are not owned by an individual and may have more than one person who knows the password.

Background

Employees of the Secretary access systems and applications through rights granted by roles. User passwords are forgotten or automatically expire by access control software and need to be reset. External customers of the Secretary need password protected access to the Secretary's systems to conduct business with the Secretary. These passwords need to be reset.

The passwords for the applications this policy includes, but are not limited to: enterprise applications, time and billing software, issue tracking software, helpdesk, and intranet.

Definitions

Term	Definition
Application Administrator (AA)	A person in the business area who is familiar with the application used by the division. The AA administers application functionality and user access.
External User	A person who is not an employee of the Secretary but does authenticate to an enterprise application of the Secretary. External user account usernames are created by the external user.

- Focused on Security. Dedicated to Success. -



User Password Policy

Internal User	A person who is an employee of the Secretary and may access both internal and external applications. Internal user accounts are derived from the agency's naming convention of first three letters of the employee's first name and the first three letters of the employee's last name.
---------------	--

Policy

Employees of the Secretary are responsible for ensuring the confidentiality and integrity of his/her personal password. All personal passwords shall never be shared. A user account can only be authorized by Division Security Officers and/or Division Management.

The owner of the personal password is the only person authorized to make the initial request to have their password reset or unlocked. The employee must be verified by an ISD staff employee and an electronic request must be submitted to have the password reset or unlocked. When the employee is at a location other than the Public Service Building, or at a location where the user cannot be verified by an ISD staff employee, the request must go through the Division's Security Officer or Division Management. All requests for password resets shall be sent to the agency helpdesk.

A temporary user password will be given to the authorized user or to the Division's Security Officer or Division Management. The user must change the temporary password immediately.

Division Directors or delegates AND the Human Resources Division (HRD) Director or delegate, may request an employee's password to be reset or locked.

Password reset requests for external users shall be submitted by the business area's Application Administrator (AA). The AA must then submit an electronic request to have the password reset. In the absence of the division AA, electronic approval shall be submitted by the division's Management.

All inappropriate requests for password resets shall be reported immediately to the requesting Division and ISD management.

The Corporation Division Security Officer will be responsible for creating all Oregon State Correctional Institute (OSCI) inmate passwords.

- Focused on Security. Dedicated to Success. -



User Password Policy

User passwords shall never be in writing or stored in an electronic format. Automated password saving tools shall not be used to save and store personal passwords.

Failure to Comply

Failure to comply with this policy may result in disciplinary action up to and including dismissal from state services for employees or termination of contracts for customers, contractors, partners, consultants, and other entities. Legal action may also be taken for violations of applicable regulations and laws.

Guidelines

- Password reset requests should be sent to the Secretary's helpdesk for documentation and auditing.
- All temporary passwords should be uniquely derived using strong password characteristics.
- Passwords should be created using strong password characteristics. The password should be a minimum of six alpha-numeric characters. Examples of strong passwords contain a minimum of two alpha and two numeric characters, and should contain at least one non alpha-numeric character, @,#,\$,%,&,*=?,!. Example: IL0vePep\$1
- Personal passwords should be changed every 90 days. When available, mechanisms are in place to enforce changing passwords every 90 days.

- Focused on Security. Dedicated to Success. -