

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Department of Revenue; Security
PROCEDURE # 6.5.5	SUBJECT: User IDs and Passwords	
EFFECTIVE DATE: 6/22/10		
CONTACT: DOR Security Office		LOCATION: State Office Building, Station #17 PHONE: 502-564-5200

STATEMENT OF AUTHORITY

1. The Finance and Administration Cabinet's Standard Procedures Manual establishes standard mandatory internal procedures cabinet-wide. These procedures are established in accordance with the Secretary's statutory authority under KRS 42.014 and KRS 12.270 to establish the internal organization and functions of the Cabinet as necessary to perform the duties effectively.
2. The Standard Procedures Manual may only be revised in accordance with the process outlined in Standard Procedure #1.1 entitled: "Finance Standard Procedures and Manual".

I. INTRODUCTION

To comply with the statutory requirements of [KRS 131.190](#) and the Internal Revenue Code (IRC) section 6103, the Department of Revenue (DOR) requires that employees shall not intentionally and without authorization inspect or disclose confidential tax information and payroll and personnel information. It is also the policy of the DOR that employees shall obtain written authorization before accessing electronic information.

The DOR Security Office shall issue a unique User Identification Number (USERID) to each employee. The USERID is used to grant access to specific computer systems to an employee. The DOR Security Office shall also assign employees a unique password that the employee must change during his or her initial logon. In addition to the automatically scheduled expiration and resetting of a password, either the employee or the DOR Security Office may change a password whenever there is a need.

II. DEFINITION

For the purpose of this policy, a DOR "employee" is defined to include all recipients of a DOR USERID, such as Department employees, Internal Revenue Service (IRS) employees, contractors, consultants, Property Valuation Administrators (PVA) and staff, or agents of the PVA and the DOR.

III. POLICY

It is the policy of the DOR that all employees' passwords are confidential and shall be treated as such. DOR employees shall be made aware of their responsibilities before obtaining access to DOR computers and data to perform their duties.

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Department of Revenue; Security
PROCEDURE # 6.5.5	SUBJECT: User IDs and Passwords	
EFFECTIVE DATE: 6/22/10		
CONTACT: DOR Security Office		LOCATION: State Office Building, Station #17 PHONE: 502-564-5200

IV. PROCEDURE

A. Employee Responsibilities

DOR employees processing or accessing confidential taxpayer data or sensitive administrative information (i.e., personnel, purchasing, and accounting data) within the agency shall follow the User ID and Password Policy ([CIO-072](#)) adopted by the DOR.

1. Change password(s) and notify your immediate supervisor or manager immediately, if it is suspected that a password has been divulged or if the password has been divulged.
2. Do not give your password to anyone, including a supervisor, under any circumstances. Should anyone request access to your password, it should be reported immediately to your immediate supervisor, manager or to the next individual in the chain of command, as determined appropriate. It is your ultimate responsibility for any password misuse.
3. If there is a breach in security, the supervisor or manager shall notify his/her Director, Executive Director, and the DOR's Commissioner or his/her designee, prior to contacting an outside agency.
4. The Commissioner or his/her designee shall then notify the Secretary of the Finance and Administration Cabinet or his/her designee and the Executive Director of the Office of Policy and Audit within 24 hours after discovery of the security breach. If the discovery of the security breach occurred on a weekend or holiday, notification shall take place during the next business day.
5. Keep all accessed information confidential. All data accessed should be considered sensitive and confidential, unless otherwise specified.

B. Revoking USERID's and Resetting Passwords

A password is set to automatically expire after 30 days and the user must enter a new password. However, DOR employees may change their passwords at any time. Instructions for changing passwords are available from the DOR Security Office.

1. The system will revoke or disable a user's access after three (3) consecutive unsuccessful attempts are made to enter a password. The user must then contact the DOR's Security Office to have the password reinstated. If the user does not know their password, the DOR's Security Office will issue a temporary password that must be changed at the initial logon.

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Department of Revenue; Security
PROCEDURE # 6.5.5	SUBJECT: User IDs and Passwords	
EFFECTIVE DATE: 6/22/10		
CONTACT: DOR Security Office		LOCATION: State Office Building, Station #17 PHONE: 502-564-5200

2. The employee shall follow the guidelines outlined in the UserID and Password Policy ([CIO-072](#)) when creating a new password.
3. The mainframe system will revoke an employee's USERID if it has not been used within 60 consecutive days. The user must then contact the DOR's Security Office to have the USERID reinstated. If the user knows their current password, the USERID can be reinstated. If the user does not know their password, the USERID will be enabled by changing the user's assigned password to a temporary password that must be changed at the initial logon. The DOR's Security Office shall confirm a user's identity prior or reinstating a user's password or issuing a temporary password.
4. When an immediate supervisor revokes an employee's USERID, because the employee is on an extended leave of absence, the supervisor shall authorize the DOR's Security Office to enable the USERID when the employee returns to work. The supervisor must submit a completed and approved Authorization to Access DOR Confidential Computer Information form ([Form SP7.605021](#)) to the DOR's Security Office with the relative START DATE." If the user knows his/her current password, the USERID can be reinstated. If the user does not know his/her password, the DOR's Security Office will enable the USERID by changing the user's assigned password to a temporary password that must be changed at the initial logon.

C. Password Construction Guidelines

DOR employees shall follow the guidelines outlined in the UserID and Password Policy ([CIO-072](#)) to construct a new password. The DOR's Security Office will instruct the user on how to change their password, if assistance is needed.

1. Mainframe passwords shall be no more than eight (8) alphanumeric characters and no less than five (5) characters (for example, Text1, 12ABC, etc.) Do not use spaces or special characters, such as punctuation marks, other than the dollar sign, pound sign or the at sign.
2. Network passwords shall be no more than 14 characters and no less than eight (8) alphanumeric characters.
3. Passwords shall not be stored in batch job control language (JCL).

Finance and Administration Cabinet STANDARD PROCEDURE		ISSUED BY: Department of Revenue; Security
PROCEDURE # 6.5.5	SUBJECT: User IDs and Passwords	
EFFECTIVE DATE: 6/22/10		
CONTACT: DOR Security Office		LOCATION: State Office Building, Station #17 PHONE: 502-564-5200

V. CONFIDENTIAL AND OTHER INFORMATION NOT TO BE DISCLOSED

Employees must maintain the confidentiality of the following types of information:

- A. Confidential taxpayer information ([KRS 131.190](#)). See the DOR Standard Procedure # 6.1.2, Confidentiality of State and Federal Information.
- B. Any other information handled or in the possession of the DOR that is determined to be of a sensitive nature, and which employees are advised.

VI. DISCIPLINARY ACTION

DOR employees are responsible for any misuse of their personal passwords. If a violation of this policy occurs, employees may be subject to disciplinary action, including reprimand, fine and dismissal.

VII. REFERENCE

Enterprise UserID and Password Policy ([CIO-072](#))

VIII. FORMS

[Form SP7.605021](#): Authorization to Access DOR Confidential Computer Information