

PERSONNEL CABINET SYSTEMS APPLICATION SECURITY

Procedures for Personnel Data/Information Access

Procedure: PERS-040.001 EFFECTIVE 01-01-08

Purpose

This document details the Personnel Cabinet Human Resource data access security procedures. Planning and provision for security will be provided by the Personnel Cabinet's Application Security Administrators located within the Department of Human Resources Administration, Division of Employee Management, Organizational Management Branch. The Personnel Cabinet adheres to security policies, standards and procedures to protect information from unauthorized, accidental, intentional, or malicious modification, destruction, or disclosure. Security must be sufficient to ensure the confidentiality, integrity, availability, and accountability of sensitive and/or critical information. The Personnel Cabinet also follows the Commonwealth Office of Technology's security standards. The Personnel Cabinet's Department of Human Resources Administration, Division of Employee Management is responsible for maintaining this security procedure. Modifications to this document must have the approval of the Commissioner of the Department of Human Resource Administration.

Application

This procedure applies to all users from the Personnel Cabinet and any other entities that access Personnel Cabinet Human Resource data. This procedure also includes vendors and / or contractors who access Personnel Cabinet Human Resource data.

Authority

KRS 11A.005 - Statement of Public Policy

KRS 11A.020 - Public Servant Prohibited from certain conduct-- Exception-- Disclosure of Personal or Private Interest

KRS11A.040 - Acts Prohibited for Public Servant or Officer --Exception

KRS 369.118 - Acceptance & Distribution of electronic Records by Governmental Agencies

KRS 434.840 - Unlawful Access to a Computer – Definitions

09-ORD-049 - Designated Information Fields

Policy Number CIO-060 - Office of the Chief Information Officer Enterprise Policy

Policy Number CIO-072 - User ID and Password Policy

Policy Number CIO-079 - Logon Security Notice

Policy Number CIO-080 - Password Auditing and Policy Enforcement for Network Domains

Policy Number CIO-081 - Securing Unattended Workstations Policy

Policy Number CIO-083 - Storage of Confidential Information on Portable Devices and Media

Cabinet Use of Technology Resources - <http://personnel.ky.gov/info/emphb/techres.htm>

e-CFR Title 45: Public Welfare, Part 164 – Security and Privacy

Personnel Cabinet Data Security Policy

Procedures

The Personnel Cabinet in partnership with agencies and other entities ensure security provisions and safeguards are in place for authorized users. The following outlines this process:

- A Memorandum of Agreement relating to accessing and use of Personnel Cabinet data (information) shall be signed by the Agency's Cabinet Secretary or Agency Head, the Commissioner of Department of Human Resources Administration and the Director of the Division of Employee Management. The MOA encompasses all Personnel Cabinet Human Resources Data Systems.

- The Agency Head/Designee shall designate a member(s) of the Agency Human Resources Administration Staff as an Agency Security Contact(s) on the Agency Security Contact(s) Designation/Removal Form.
 - If the Agency Head/Designee *is* the Agency Security Contact (i.e.: Boards and Commissions) and therefore *must* request their own access and/or increase in authority; they must complete an Exception Request letter to the Director of the Division of Employee Management for approval.
- All Designated Agency Security Contacts are required to sign an Agency Security Contact Agreement which allows them to request access to any Personnel Cabinet Human Resource Data Systems for users in their agency.
- Designated Agency Security Contacts are responsible for requesting access for specific staff to Personnel Cabinet systems. Designated Agency Security Contacts shall provide to the Personnel Cabinet's Application Security Administrator an electronically signed Authorized Agency User Security Agreement for each user identified as requiring access to Personnel Cabinet Systems.
- Designated Agency Security Contacts will complete the appropriate User Access Request Form for each employee requiring access. Access Request Forms for each user must be sent in an individual email. The form must be sent to PER.S.KHRIShelpdesk@ky.gov by the Designated Agency Security Contact.
- Any missing information, incorrect access levels, or any other item not accurately reflected on the User Access Request Form will result in the Form being returned for correction.

Designated Agency Security Contacts and the Personnel Cabinet Application Security Administrators will ensure access to Personnel Cabinet Human Resource data is current. Once a month the Designated Agency Security Contacts will review the PERPOPA2 report, and if there are any users who no longer require the access listed on the report or if a user's access should be deactivated or modified, then submit the appropriate User Access Request Form, to change access as required. The PERPOPA2 report monitors all employees in the agency utilizing CICS and what access they currently have. The report is updated each weekday morning and can be found on Document Direct.

No one may submit a User Access Request Form requesting access or an increase in authority for themselves for their own ID. For example, if the request is for a Designated Agency Security Contact, then an Agency Head/Designee or a Designated Security Contact must email the form with their name in the "Requestor" field.

-The only exception to this rule is if the Agency Head/Appointing Authority *is* the Designated Agency Security Contact and the exception request, previously sent to the Director of the Division of Employee Management, was approved.

Access to a Personnel System may be provided upon electronic receipt of the User Access Request Form. This electronic copy will serve as the official record and must be sent from the Designated Agency Security Contacts electronic mailbox. When required the Personnel Cabinet will provide new users their login credentials via email. Upon the first login, the new user will be prompted by the system, on the second screen after login, to change their password. The user's password must adhere to standards for each system. The Personnel Cabinet's Application Security Administrators will process the request from the Agencies in a timely manner. Other security settings and procedures will be addressed for each system. Wherever possible, these will be standardized.