

## University of Kansas Human Resource & Equal Opportunity Systems and Data Usage

**Storing/Saving Data** - No confidential data (including HR/Pay data) is to be stored on any unsecured device, this includes but is not limited to USB drives, disks, cds, hard drives etc.

- [Fraud and Theft Prevention Policy](https://documents.ku.edu/policies/Chancellor/FraudandTheft.htm) (https://documents.ku.edu/policies/Chancellor/FraudandTheft.htm)
- [Privacy & Security of Information Tips](http://www.privacy.ku.edu/docs/FinalTips.pdf) (click on link [www.privacy.ku.edu/docs/FinalTips.pdf](http://www.privacy.ku.edu/docs/FinalTips.pdf) )
- [Fraud and Theft Prevention Policy](https://documents.ku.edu/policies/Chancellor/FraudandTheft.htm) (click on link <https://documents.ku.edu/policies/Chancellor/FraudandTheft.htm> )
- [Records Retention](http://www.comptroller.ku.edu/documents/records_retention.pdf) (click on link [www.comptroller.ku.edu/documents/records\\_retention.pdf](http://www.comptroller.ku.edu/documents/records_retention.pdf) )

**Use of HR/Pay Data** - data extracted or originated from the HRSA system or DEMIS HR/Pay is not to be released or used with other systems without the written authorization from the Director of HR/EO or his/her designee. Some data may also require the additional authorization of the Director of Payroll and/or Comptroller.

The request should include the

1. purpose of the release or use,
2. security of the data,
3. who will be accessing the data and
4. data fields that are being used.

HR/EO may request a security audit to be sure the method of transferring the data complies with University of Kansas Security Standards before the approval of data may be given.

**Access to HR/Pay Data** - Access to HRSA (which is the PeopleSoft HR/Payroll database) is granted for those with job responsibilities related to HR/Payroll activities. Employees must attend training which is generally offered monthly and varies from 1/2 day to 3 1/2 days based on job responsibilities. HR/Pay data (HRSA) is not to be accessed over a wireless connection. [www.hreo.ku.edu/training/info/course\\_details/58](http://www.hreo.ku.edu/training/info/course_details/58).

**Access to PeopleAdmin** - Administrative Access (Hiring Manager) (is a hosted site for posting position descriptions and vacancies) is granted after attending training which is generally held twice a month. Applicants do not have to attend training. [www.hreo.ku.edu/peopleadmin/hiring\\_manager\\_tr.shtml](http://www.hreo.ku.edu/peopleadmin/hiring_manager_tr.shtml).

**User ID and Passwords** - Database information, particularly personnel and search information is COMPLETELY CONFIDENTIAL. Employees will be required to attend training and sign a statement that they will not share or authorize the use of their User ID before access will be granted to HRSA or PeopleAdmin and related DEMIS systems. If a user shares their signon or allows another to use their access after signing on either of these are considered to be a security violation which will result in the revocation of his/her access and notification to his/her supervisor. Users must also agree to comply with the policies of the University of Kansas regarding the proper use of computing resources. Knowingly releasing or misusing confidential information from official records may result in disciplinary action up to and including dismissal.

The Password policy is located at [https://documents.ku.edu/policies/Information\\_Services/Password.htm](https://documents.ku.edu/policies/Information_Services/Password.htm). HRSA (PeopleSoft) has unique rules regarding passwords. You must have all 4 items below.

1. Must be 7 or 8 characters long but *cannot be longer than 8 characters (but must be 7 to comply with the University policy)*.
2. The leading character must be an upper case alphabetic character (A-Z). *Alphabetic characters keyed are automatically converted to upper case when signing in to HRSA.*
3. Must include one of the following three special characters #, \$, \_. *Only three special characters are allowed, if you use others the new password will not be changed or saved.* (The KU policy allows additional special characters but HRSA PeopleSoft does not so you are only allowed to use the 3 listed above.)
4. Must include at least one digit (0-9).

Therefore, users are to create a 'strong' password that is 7 or 8 characters long. It must include at least one of the three special characters and at least one digit (0-9) and begin with an upper case alphabetic character.

### Related Document:

HR/Pay Wireless and Remote Access Use and Data Storage

[www.hreo.ku.edu/files/documents/Wireless\\_VPN\\_Storage\\_HRPAY.pdf](http://www.hreo.ku.edu/files/documents/Wireless_VPN_Storage_HRPAY.pdf)