HR POLICY

King County
Department of Human Resources

Employment Data Security Policy

Policy Number: 2024-0001
Issue Date: 9-20-2024

PURPOSE

King County is committed to securing, protecting, and keeping private the employment data contained in its Human Resources (HR) systems of record. The purpose of this policy is to ensure that access to employment data is assigned, managed, and monitored in a controlled manner and only accessed on a "need-to-know" or "right-to-know" basis.

APPLICABILITY

The County's *Employment Data Security Policy* applies to the executive branch departments, offices, and divisions, including the Assessor's Office and King County Elections.

DEFINITIONS

"Advanced PeopleSoft Security access" means any access beyond an employee's base Self-Service or Manager Self-Service level.

"Employment Data" means any information or record about a person that is obtained in the context of that person's employment, or potential employment, with the County. Such persons include job applicants, current and former employees, as well as any family members of such persons.

"Need-to-Know" means the standard of obtaining or accessing employment data for the purpose of fulfilling official job responsibilities, as determined by King County.

"PeopleSoft" means King County's Human Resources management software system of record.

"Right-to-Know" means the standard of obtaining or accessing employment data pursuant to rights spelled out in federal, Washington State, or King County law.

"Security or Privacy Incident" means an event that may lead to the loss of confidentiality, integrity, or availability of data.

"System of Record" means any of the centralized software systems that collect and store employment data. Examples of official systems of record include, but are not limited to: PeopleSoft, NEOGOV, Origami, and Laserfiche.

"Third-Party Access" means the process of the County granting system of record access to external vendors and service providers for any purpose.

POLICY

King County creates and maintains employment data, which can include personally identifiable information, for the purpose of conducting county business and supporting the County's workforce.

King County shall only collect employment data that is directly relevant and necessary for accomplishing specific human resources functions and shall take steps to ensure that employment data is accurate, complete, and kept up to date.

Access to systems of record includes permission to view sensitive, confidential, and personally identifiable information related to King County employment. Therefore, access to these systems shall only be granted to employees with a job-related need for such access.

Access to systems of record shall be controlled to ensure that the information contained in these systems is used appropriately, responsibly, and in compliance with the King County Code of Ethics and other related policies.

The Department of Human Resources shall retain employment data only for the minimum amount of time necessary to conduct county business in accordance with approved records retention schedules and shall dispose of employment data in a manner that is secure and prevents unauthorized disclosure.

Employment Data and Public Records Requests

Employment data contains information relating to the conduct of King County government and the performance of its functions. Therefore, employment data are public records. The County's responsibility to secure employment data shall be balanced with the public's "right-to-know" found in Chapter 42.56 RCW (the "Public Records Act"), King County Code 2.14.030, and all other applicable federal, state, or local laws.

Access to Employment Data and Systems of Record

Department Usage: Departments shall obtain approval from DHR prior to using employment data derived from a system of record in department-specific side systems, data repositories, or data interfaces. This requirement does not apply to Peoplesoft queries or certain longstanding, department-specific HR systems.

Third-Party Access: Departments shall obtain approval from the DHR Director or designee prior to granting third-party access to systems of record. Third party access requests will be evaluated by DHR on a case-by-case basis; however, approval will be limited only to situations where third parties use employment data to conduct non-regular county work, i.e., ad hoc special projects, etc.

PEOPLESOFT PROCEDURES

Only employees designated by their supervisor and authorized by their Department Security Officer (DSO) may have access to advanced PeopleSoft security. Employees who access PeopleSoft will be held responsible for protecting and preventing unauthorized access to the system, protecting confidentiality, and providing employment data only to persons on a "right-to-know" and "need-to-know" basis.

When necessary and supported by a business need, new job responsibilities may be created, or existing job responsibilities may be modified to include advanced PeopleSoft security. The creation or modification of a PeopleSoft security job responsibility shall be subject to "need-to-know" and "right-to-know" criteria.

PeopleSoft Advanced Security Access Request Process

The chart below outlines the advanced PeopleSoft security access request process for employees with access needs that are beyond Self-Service or Manager Self-Service levels.

1.	Employee	Access PeopleSoft, navigate to: Employee Self Service > My Security > Advanced Access Requests > Create Security Request
2.	Department HR Teams	Access PeopleSoft, navigate to: Workforce Administrator > Department Security > My Position Security Requests > Create Request
3.	Department Security Officer	Approve or deny the request based on a "need-to-know" standard. If the standard is not met, the request will be returned to the originator.
4.	PeopleSoft	Security applied to position number nightly via KC_AP_SEC_AE.

Auditing Advanced PeopleSoft Security Levels

Each March and October, the Department Security Officer will run the following audit reports:

- **KC_SEC_TLGROUP_POSN,**
- **KC_SEC_DEPT_POSN, and**
- **KC_SEC_JOB_RESP_POSN**

Updates will be made, as needed, and communicated to affected employees, their supervisor, and the Department HR Manager.

Each March and October, DHR will run the following audit reports to ensure "need-to-know" standards are appropriate:

- **KC_SEC_TLGROUP_POSN,**
- **KC_SEC_DEPT_POSN,**
- **KC_SEC_JOB_RESP_POSN,** and
- **KC_SEC_COUNTY_ACCESS**

DHR will make the appropriate updates, as needed, and communicate them to affected employees, their supervisor, the Department HR Manager, the Department Security Officer, and the DHR Service Delivery Division Director.

RESPONSIBILITIES

The Department of Human Resources is responsible for:

- Taking the appropriate measures to secure employment data stored in systems of record;
- Maintaining an employment data breach response plan compliant with the County's Incident Response Policy;
- Ensuring appropriate training for end-users is provided and modified, as needed;
- Overseeing and conducting a regular cycle of scheduled audits; and
- Supporting the Business Resource Center during annual audits.

The Business Resource Center is responsible for ensuring technology meets business standards and policies.

Departmental HR Managers are responsible for ensuring:

- Departmental Security Officers complete all required training;
- Departmental Security Officers approve or deny job responsibility, department ID, or Time & Labor Group security levels requests in accordance with this policy; and
- Regular auditing is completed and documented.

Department Security Officers are responsible for understanding each job responsibility, department ID, Time & Labor Group, and how they apply to each position's "need-to-know" standard. Department Security Officers shall review security requests, give final approval before security is applied, and are responsible for responding to BRC audit findings. The DSO will complete department auditing every March and October and is required to complete annual training.

Departmental HR teams are responsible for having a general knowledge of each job responsibility, department ID, and Time & Labor Group to be able to advise supervisors and/or other employees on necessary "need-to-know" standards related to each position. HR Teams will review position security prior to an individual being placed into a position to ensure their security level is appropriate.

Supervisors are responsible for engaging with their Human Resources team, Timekeeper, or Security Officer to consult on which job responsibility, department ID, and/or Time & Labor Group is needed to perform the assigned tasks of the positions that report to them.

All system of record users are responsible for following this policy as well as all applicable King County IT Policies. To access a system of record, users must engage with their supervisor, Human Resources team, Timekeeper, or Department Security Officer to request the appropriate security necessary for their position or to verify their existing position security is still valid.

REFERENCES

King County Code of Ethics

King County Data Security Policy

King County Privacy Notice

Information Security Policy and Standards Glossary

PeopleSoft Resources (links must be accessed via VPN)

PeopleSoft Advance Security Job Responsibilities

PeopleSoft Department Security Officer Checklist

PeopleSoft Department Security Officer User Guide

PeopleSoft Human Resource Position Requestor Security Guide

QUESTIONS

Refer questions to the Department of Human Resources.