Annual HRMS User/Position Audit

The OFM HRMS Security Team is initiating a yearly HRMS User/Position audit and will be contacting each agency designated HRMS Security Requestor. The notification to the Security Requestors will have instructions and resources available for use to complete the audit.

To help streamline the process for agencies:

- The HRMS Security Team has enhanced the agency Security Reporting roles that will provide reports to find the agency positions that have HRMS roles assigned and holders of those positions.

- For this yearly audit agencies will be allowed to send a single request to OFM HRMS Security for role removals. The standard HRMS Role Request form for each position change will not be required.

If you don't know your agency designated HRMS Security Requestors, contact heretohelp@ofm.wa.gov and they can provide the names.

It is important that agency Security Requestors work with their HR/Payroll Office to verify current position information. Security Requestors should also work with the supervisor of the position and verify if the position responsibilities require the assigned HRMS roles and license.

Example:
- Holder leaves HRC3 position that is assigned the HRMS Personnel Admin. Processor role.
- Organization reviews the use of the position and decides to redeploy and fill as a DEI consultant.
- The responsibilities of the position no longer require HRMS access.
- The agency Security Requestor submits the request to remove the HRMS role from the position. This will also free up the HRMS license held by the position.

OFM is responsible for managing HRMS license usage and relies on agencies to actively and accurately manage HRMS access. Paying for unused HRMS licenses takes funds away from other critical enterprise services and technology.

LTSS Implementation Update

Current Activities:
- OFM continues to work with ESD to clarify requirements for finalizing system and business process changes.
- After notice was given to unions on May 5th, State Labor Relations received demands to bargain. They are in discussions with the unions that submitted demands.
- LTSS rule making is in progress:
  - Phase One Exemption Rules have been finalized.

- ESD has not shared the business process for requesting exemptions at this time.
    - o Phase Two - Premium collection, CBA exemption, election of coverage, refunds, reporting and payments, appeals still *draft*
    - o Phase Three - Determinations of "qualified individual" status, audit functions, designated representatives *pending*
- OFM is drafting a standard communication for agencies and institutions to communicate the new premium tax to employees. ESD has additional employee communication resources:
    - o WA Cares Fund website: http://www.wacaresfund.wa.gov/employers/?utm_medium=email&utm_source=govdelivery
        - Employer tool kit has downloads for use - key messages and a program infographic
    - o Sign up for the ESD Employer Newsletter via GovDelivery. Subscription link is on the webpage. The first edition was sent Thursday, May 27.

Reminder: Sharing Workforce Data & Data Sharing Agreements

With the implementation of SB 5432 Concerning cybersecurity and data sharing in Washington state government (effective 7/25/21) when sharing personally identifying information (PII), also known as category 3 & 4 data, agencies must establish a data sharing agreements. This includes when sharing data between general government agencies and/or higher education institutions. For example, if the State Auditor's Office is conducting an audit and requests employee data that includes social security numbers, name and date of birth, this combination of data is considered category 3 data and a data sharing agreement must be executed. The law does not limit the ability of the State Auditor's Office to conduct audits, it does require a DSA if category 3 & 4 data is included.

When requesting data from partner agencies that require a DSA, please be sure to build the time it takes to execute a DSA into your request timeline.