

WorkforceOne Security Administrator (SA) Responsibilities

Security Administrator I (SA I)

Security Administration I level exists only at the Internal Security Office at the Department of Employment and Economic Security (DEED). The SA I staff will have no access to customer (Person Record) information in Workforce One. The SA I level responsibilities will include:

Setting policy for enforcing data privacy.

- Developing forms for requesting access to the system.
- Approving staff for the SAII level and assigning the SAII access privileges to a staff record.
- Monitoring activity at the Security Administration II levels.
- Managing the Security Access for users in selected Data Regions.
- Approving staff for the state level "Record Manager" privileges and assigning the privileges to a staff record.
- Approval or denial of user requests for access to Workforce One data based on legitimate business need and applicable laws and policies.
- Maintain user access request forms for verification, and auditing purposes.
- Inactivate user access at time of employment termination.

Security Administrator II (SA II)

Security Administration II level may be appointed for local WF1 data regions where there is frequent security administration activity. For those regions it is expected there will be one SA II, and a back-up trained. A training class in WF1 security administration is required before the privileges will be granted. The responsibilities will include:

- Managing the Security Access for all Staff (users) in their data Region.
- Ensuring the Data Privacy Laws and Policies regarding Workforce One data are enforced at the Region level.
- Approval or denial of user requests for access to Workforce One data based on legitimate business need and applicable laws and policies.
- Maintain user access request forms for verification, and auditing purposes.
- Inactivate user access at time of employment termination.

The staff person appointed to security administration positions should:

1. Have first hand knowledge of new Agencies contracting with the Region and Agencies no longer contracting with Region.
2. Be available for quickly processing requests for user access to the system.
3. Should have minimal conflict of interest in protecting the data versus accessing records for other job responsibilities.
4. Should be a trusted employee who will have the authority to deny a user access to data not needed for the performance of their program administration functions.

Security Administrator III (SA III)

Security Administration III level may be appointed for local WF1 agencies within data regions where there is frequent security administration activity. For those agencies it is expected there will be one SA III, and a back-up trained. A training class in WF1 security administration is required before the privileges will be granted. The responsibilities will include:

- Managing the Security Access for all Staff (users) in their agency.
- Ensuring the Data Privacy Laws and Policies regarding Workforce One data are enforced at the Region level.
- Approval or denial of user requests for access to Workforce One data based on legitimate business need and applicable laws and policies.
- Maintain user access request forms for verification, and auditing purposes.
- Inactivate user access at time of employment termination.

The staff person appointed to security administration positions should:

1. Have first hand knowledge of the Agency and locations.
2. Be available for quickly processing requests for user access to the system.
3. Should have minimal conflict of interest in protecting the data versus accessing records for other job responsibilities.
4. Should be a trusted employee who will have the authority to deny a user access to data not needed for the performance of their program administration functions.