Attachment

Internal Security Guidelines for Unemployment Insurance Programs

UI program administrators must ensure that continuing efforts are in place to discourage, prevent, and detect incidents of employee fraud, waste, and abuse in UI program operations. Safeguarding UI assets includes providing employee training to strengthen the awareness of potential fraud, waste, and abuse in the UI program. The awareness and training should include procedures that are employed by the state to prevent unauthorized access and use of confidential UI information. Both claimant and employer information must be protected to maintain program integrity. Separation of duties within and between benefits and tax operations and within specified functions or operational areas is an essential criterion in mitigating internal fraud and/or abuse.

Below are some guidelines for Internal Security controls and integrity procedures. The guidelines listed below are <u>not</u> all-encompassing. States should develop additional guidelines to fully satisfy their individual Internal Security requirements and ensure that employees and contract staff are aware of the requirements.

General Guidelines

- No employee shall trace, attempt to duplicate, or otherwise forge the signature of a claimant, applicant, program participant, employer, or other state employee on any UI, employment service, or other state document.
- No employee shall assist or encourage a claimant or employer to provide misinformation or take any dishonest or illegal actions with the intent of improperly affecting the status of a claimant, applicant, or employer.
- No employee shall make an unauthorized alteration to any document or modify any electronic/system information that would improperly affect the eligibility or status of a claimant, applicant, program participant, or employer concerning a state or Federal UI program.
- No employee shall establish a personal bank account for the purpose of accepting and remitting tax receipts, benefit repayments, or any receivable processed by the state for deposit into any UI trust fund account.

Conflicts of Interest

- No employee shall participate in providing any UI service to a relative or friend. Examples include but are not limited to filing, adjudicating, or paying a claim; performing an eligibility review interview; taking an employment service application and providing selection and referral to jobs; conducting an appeals hearing; conducting a tax audit; or referring to training or special programs. A relative means any of the following related to the employee by blood, marriage or adoption: spouse, children, parents,

grandparents, sisters, brothers, aunts, uncles, nieces, nephews, cousins, in-laws and step-relatives.

- No employee shall hold any outside employment/interest or provide personal services for a business which constitutes, or appears to constitute, a conflict of interest with the employee's work responsibilities.
- No employee, in return for the performance of his/her official duties, shall request or accept from any person any gratuity, reward, or other consideration.

UI Benefit Operations

- No employee shall provide information to claimants, within or away from the office, which can be used to improperly obtain benefits through misrepresentation and/or false information to avoid suspension, reduction of benefits, or disqualification on a claim.
- No employee shall change a claimant's address without authorization from the claimant and without having the responsibility and authority to do so.
- No employee shall request that claimants disclose their Personal Identification Number (PIN) or sign blank forms, such as initial claims forms, continued claim certification forms, address change forms, etc.
- No employee shall backdate a UI claim, if permitted under state law, without authorized approval and unless it is in accordance with the state's policies and procedures.
- No employee shall transfer a claim retroactively from one UI program to another without approval of authorized personnel/manager.
- No employee shall certify and/or pay a claimant that files an untimely UI continued claim certification(s) without authorized approval; and the action must be in accordance with the state's policies and procedures.
- No employee shall change or defer a claimant's employment service registration requirement or mandatory participation in reemployment services except where permitted under state UI law or policy and where authorized approval exists to do so.

UI Tax Operations

- No employee with data entry privileges to a state's automated system shall enter any transaction on an employer's account without having authority and justification to do so.
- No employee shall establish or terminate an employer's liability, change an address, adjust, waive or cancel amounts due, or adjust unemployment experience and/or tax rates on an employer's account without having the authority to do so, and action(s) must be carried out in accordance with the state's policies and procedures.
- No employee shall advise an employer on how to evade proper charges related to a claim.
- No employee shall request that employers disclose their PIN or sign blank forms, such as employer registrations, contribution and wage reports, change of address, or power of attorney forms.

Information Security

- No employee shall display his/her username or password information in a manner that will allow unauthorized access to any state information system.
- No employee shall share his/her username or password information with another individual to access any state information system.
- No employee shall expose claim information or make it vulnerable to public view.
- No employee shall leave his/her computer unattended while logged onto the network, or while using applications that display or have access to sensitive data including personally identifiable information (PII) such as social security numbers, names, addresses, and phone numbers.
- No employee shall use claimant, employer, or state staff information or data outside the individual's normal UI job duties. Examples of information and data include PII, employment information, tax information, or other UI-related information gathered from individuals, other agencies, or other government computer systems.
- No employee shall remove any state property, including claimant, applicant, or employer source documents or electronic data, from the workplace unless authorized by management in the performance of his/her job duties and level of responsibility.
- No employee shall access, disseminate or dispose of any data created by the state workforce agency, and/or any data procured, shared or exchanged by agreement (including data shared through a Memorandum of Understanding or Memorandum of Agreement) except as authorized under the applicable federal laws, state laws, regulations and/or policies of the entity that has the proprietary interest in the data.
- No employee shall use UI data except as allowed under the applicable federal laws, state laws, regulations, and policies of the state.