COMPUTER USE POLICY:

SECTION ONE - PROHIBITED COMMUNICATIONS

Electronic media cannot be used for knowingly transmitting, retrieving, or storing any communication that is:

1. Discriminatory or harassing;
2. Derogatory to any individual or group;
3. Obscene, sexually explicit or pornographic;
4. Defamatory or threatening;
5. In violation of any license governing the use of software; or
6. Engaged in for any purpose that is illegal or contrary to WorkNet policy or business interests.

SECTION TWO - PERSONAL USE

The computers, electronic media and services provided by WorkNet are primarily for business Use to assist employees in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

SECTION THREE - SOFTWARE

To prevent computer viruses from being transmitted through the company's computer system, unauthorized downloading of any unauthorized software such as games, etc. is strictly prohibited. Only software registered through WorkNet may be downloaded. Employees should contact the system administrator if they have any questions.

SECTION FOUR - SECURITY/APPROPRIATE USE

A. Employees must respect the confidentiality of other individuals' electronic communications. Except in cases in which explicit authorization has been granted by company management, employees are prohibited from engaging in, or attempting to engage in:

   1. Using other people's log-ins or passwords; and
   2. Hacking or otherwise obtaining access to systems or accounts they are not authorized to use;
   3. Breaching, testing, or monitoring computer or network security measures;
   4. Monitoring or intercepting the files or electronic communications of other employees, clients, or third parties.

B. No e-mail or other electronic communications can be sent that attempt to hide the identity of the sender or represent the sender as someone else.

C. Electronic media and services should not be used in a manner that is likely to cause network congestion or significantly hamper the ability of other people to access and use the system resources.

D. Anyone obtaining electronic access to other companies' or individuals' materials must respect all copyrights and cannot copy, retrieve, modify or forward copyrighted materials except as permitted by the copyright owner.

SECTION FIVE - ENCRYPTION

Employees can use encryption software supplied to them by the system's administrator for purposes of safeguarding sensitive or confidential business information. Employees who use encryption on files stored on a company computer must provide their supervisor with a sealed hard copy record (to be retained in a secure location) of all of the passwords and/or encryption keys necessary to access the files.

SECTION SIX - PARTICIPATION IN ONLINE FORUMS

Employees should remember that any messages or information sent on company-provided facilities to one or more individuals via an electronic network—for example, Internet mailing lists, bulletin boards, and online services—are statements identifiable and attributable to WorkNet. As such only Staff designated in writing by WorkNet Management shall be allowed to e-mail / post messages to any such medium seen by the general public.

Employee Signature: _____ Date: _____

Individual Non-Disclosure and Confidentiality Certification Form

I understand that I will or may be exposed to certain confidential information, including but not limited to, personally identifying information of individuals who receive public assistance, employment and unemployment insurance records maintained by the Agency for Workforce Innovation, made available to my employer, for the limited purpose of performing its duty pursuant to a Contract for Services and Non-Disclosure and Confidentiality Certification agreement.

These confidential records may include name (or other personally identifiable information), social security numbers, wage and employment data and public assistance information which are protected under federal and state law. Such information is confidential and may not be disclosed to others. In order to perform my duties associated with the program requirements set forth under contract or agreement, I am requesting an approved username, password, and additional instructions for accessing the One Stop Management Information System (OSMIS) or the One Stop Service Tracking (OSST) system, (hereinafter collectively referred to as "the Workforce Systems"). Prior to receiving such means of access, I acknowledge and agree to abide by the following standards for the receipt and handling of confidential information:

1. I shall use access to the Workforce Systems only to secure information to conduct official program business under such contract/agreement.
2. I shall not disclose my username, password, or other information needed to access the Systems to any party nor shall I give any other individual access to information secured.
3. If I should become aware that any other individual – other than an authorized employee – may have obtained or has obtained access to my username, password, or other information needed to access the Workforce Systems, I shall immediately notify the Regional Workforce Board Security Officer.
4. I shall not share with anyone any other information regarding access to the Systems unless I am specifically authorized by the AWI.
5. I shall not access or request access to any social security numbers, personal information, wage or employment data unless such access is necessary for the performance of my official duties.
6. I shall not disclose any individual data to any parties who are not authorized to receive such data except in the form of reports containing only aggregate statistical information compiled in such a manner that it cannot be used to identify the individual(s) involved.
7. I shall retain the confidential data only for that period of time necessary to perform my duties. Thereafter, I shall either arrange for the retention of such information consistent with federal or state record retention requirements or delete or destroy such data.
8. I have either been trained in the proper use and handling of confidential data or I have received written standards and instructions in the handling of confidential data from my employer or AWI. I shall comply with all confidentiality safeguards contained in such training, written standards, or instructions, including but not limited to, the following: a) protecting the confidentiality of my username and password; b) securing computer equipment, disks, and offices in which confidential data may be kept; and c) following procedures for the timely destruction or deletion of confidential data.
9. I understand that if I violate any of the confidentiality provisions set forth in the written standards, training, and/or instructions I have received, my user privileges may be immediately suspended or terminated. I further acknowledge that applicable state and/or federal law may provide that any individual who discloses confidential information in violation of any provision of that section may be subject to a fine and/or period of imprisonment and dismissal from employment. I have been instructed that if I should violate the provisions of the law, I may receive one or more of these penalties.
10. Should I have any questions concerning the handling or disclosure of confidential information, I shall immediately ask my supervisor and be guided by his/her response.

Employee Signature: _____ Date: _____

Print Employee Name: _____

Address: _____

_____

Work Telephone: _____ E-Mail: _____