Fresno County Workforce Investment Board

2035 Tulare Street, Suite 203 ● Fresno, CA 93721 ● (559) 266-3742 ● Fax (559) 233-9633 ● www.jobsfresno.com

Blake Konczal, Chief Executive Officer

OPERATIONAL DIRECTIVE

FCWIB OD # 32-02 **Date: December 16, 2002**

To: All Fresno County Workforce Investment Board (FCWIB) Providers of Services

From: Blake Konczal, Chief Executive Officer

Effective Date: December 16, 2002

Subject: Confidential Information

Attached to this Operational Directive is the Staff Confidentiality Statement (Revised 10-27-01 as Attachment I) **that must be signed by all Providers of Services' staff/employees (Temporary, Contracted, and Part-Time or Full-Time) and/or any individual having access to confidential information, and then signed by their immediate supervisor.**

The original Staff Confidentiality Statement must be retained in the employee's personnel file. The employee must be provided with a copy of the fully executed and dated statement.

This Operational Directive supersedes FWDB/FAWIC Policy Bulletin 1-99 dated January 7, 1999. It contains **important federal and state necessary requirements** relating to all FCWIB contracted Providers of Services and their staff.

The protection of confidential information requires special precautions that include a Confidentiality Statement being signed by all Providers of Services' staff as required below. The statement restricts the unauthorized use, access, disclosure, modification, and destruction of confidential information. Providers of Services and One-Stop Partners will exchange various kinds of personal information, which may include but is not limited to job seeker and employer customer data, applications, program files, and databases. All data **and** information are confidential.

I. Background and Definitions

A. Personal Information:

All personal information associated with an individual or business includes both identifying information (e.g., name, social security number, Tax I.D. number, E-mail

address, or agency assigned case number) and nonidentifying information (e.g., age, finances, and gender). This includes all information in a customer's file and any information managed and/or stored in a computer database or system of records (e.g., case management computer software and/or case notes).

B. Collection of Information:

The Privacy Act of 1974 (as amended) is the primary act regulating the use of personal information. It places limitations on the collection, disclosure, and use of personal information maintained in systems of records. For the purposes of this Operational Directive, a "System of Records" is a group of records (computer based software or hard copy file) under the control of a Provider of Services from which information is retrieved or identified by the name of the individual or some identifying number, symbol or other particular assigned identifying term or phrase.

C. Applicable Data Source(s):

Data and/or information may be received directly from a customer, internally, another FCWIB Provider of Services, or from a federal, state, or local agency such as the Employment Development Department, California Department of Social Services, California Department of Education, County Welfare Department(s), County IV-D Director's Office of Child Support, Office of the District Attorney, California Department of Mental Health, California Office of Community Colleges, and the Department of Alcohol and Drug Programs. Data and information may also originate from an employer.

II. Requirements of FCWIB Providers of Services

All FCWIB Providers of Services must:

A. Keep in the strictest of confidence all information that is exchanged between them and outside authorized agencies or employers, and make such information available to only authorized employees on a **"need to know"** basis.

B. Not disclose any confidential information to a third party, unless a signed and current release of confidential information has been received that includes written instructions, the identification of all parties, and describes the confidential nature of the information to be released together with notice of the penalties for unauthorized use or disclosure.

C. When applicable, store and process information in electronic format in such a way that unauthorized persons cannot reasonably retrieve the information by means of a computer, remote terminal, or other method.

D. Promptly return to the other party confidential information when its use ends, or destroy the confidential information utilizing an approved method of destroying confidential information (e.g., shredding, burning, or certified or witnessed destruction). Magnetic media are to be degaussed, returned to the other party, or deleted from a computer database.

E. When entering into a third party agreement when services are to be provided, the agreement must include an assurance that each party will act in accordance with the requirements of this Operational directive and applicable law. In no event shall said

information be disclosed to any individual outside of that third party's authorized staff, without expressed written authorization.

F. Designate an employee who shall be responsible for overall security and confidentiality of its data and information systems.

G. Have a dated and signed Confidentiality Statement in each staff person's personnel file in accordance with these requirements. This applies to **all staff**, regardless of job title or current job description.