City of RICHMOND WDB Workforce Development Board	**OPERATIONS BULLETIN** **WORKFORCE INNOVATION AND OPPORTUNITY ACT**	**Policy Number ETP 04-0612** CORWDB Board Approval DATE: June 14, 2012 REVISED: July 2016 Pg. 1 of 1

Personally Identifiable Information
SECURE DATA TRANSFER POLICY

This policy is developed and maintained in accordance with the Privacy Act of 1974, Information Practices Act of 1977 (Title 1.8 [commencing with Section 1798] of Part 4 of Division 3 of the Civil Code), Sections 11015.5 and 11019.9 of the Government Code, and Sections 1094 and 1095 of the California Unemployment Insurance Code.

The City of Richmond, Employment and Training Program (CRETP), Workforce Development Board secures all client personal information against loss, damage, modification, unauthorized access, or disclosure as required by federal and California Law, and the State Workforce Development Administrative Manual policy. Information voluntarily provided by the client will be protected by the appropriate computer, network, and Internet technical security controls at the employee and departmental level to prevent unauthorized access. Some of these security controls are: password and user identification verification, data encryption, confidential transmissions, secure storage areas, and audit trails.

The CRETP does not store or use personal information submitted by the client any longer than necessary. If no longer required and in order to prevent unauthorized access or use of the data, the client's personally identifiable information is destroyed via purging, magnetic degaussing/erasing, shredding and/or other means of authorized confidential destruction. Regularly scheduled archiving, purging, and proper disposal of records and information are a standard practice throughout the City of Richmond local government agency.

The CRETP employees will only use personal information submitted by the participant as it relates to eligibility for providing program services. CRETP employees are educated regarding the requirements of working with confidential and personally identifiable information as well as the consequences of misuse. CRETP employees will attend mandatory yearly reviews of all acts, policies, and codes relating to protecting Personal Identifiable Information. CRETP will not sell or distribute personal information to any non-governmental entity without the client's consent or as authorized by law or regulation.

All CRETP data transmissions of PII will require prior approval by administrative staff and will be severely scrutinized and approved on a case-by case basis. CRETP Director and Fiscal Manager will be responsible for ensuring that no PII data be transmitted without prior encryption in accordance with FIPS 140-2.

As a public agency, the CRETP understands the importance of maintaining the client's privacy and will make every attempt to maintain their confidence and trust regarding the collection and use of personal information.