RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

Provider Name: State of California, Employment Development Department

Date Requirements retrieved: March 7, 2016
Source Requirements retrieved from:
http://www.dgs.ca.gov/ols/Resources/StandardContractLanguage.aspx

Standard Agreement, # M6102380
Exhibit A (Secure File Transfer)
Exhibit E "Special Conditions for Security of Confidential Information"
Section I (Administrative Safeguards)
Section II (Management Safeguards)
Section III (Usage, Duplication and Redisclosure Safeguards)
Section IV (Physical Safeguards)

#	Requirement	Met? (Yes/No)	Notes
A/ II/ 2a	A limit of five attempts to enter the password after which the account will be locked. To request User Account support submit an email message to: Aileen.Douglas@edd.ca.gov	Yes	
A/ II/ 2b	Retrieve the response data file from the SFT temporary file storage repository within twenty (20) calendar days from submission. On the 21th day, the data file is automatically deleted.	Yes	
A/ II/ 2c	Comply with the California Unemployment Insurance Code (CUIC) on any matters pertaining to the access, use, and/or release of data under this agreement. Failure to comply with this provision shall be deemed a breach of this agreement and shall be grounds for cancellation of this Agreement.	Yes	
A/ II/ 2d	Oversee the UCSB staff in their use of confidential information received from the EDD.	Yes	
IV/ a	Take precautions to ensure that only authorized personnel are given access to physical, electronic and on-line files. Store electronic and hard copy information in a place physically secure from access by unauthorized persons. Process and store information in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot retrieve the information by means of computer, remote terminal, or other means.	Yes	Project media stored in fire safe with combination lock inside of "High Security" area of North Hall Data Center (access controls via keycard, staffed 8 hours daily and alarmed)

RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

IV/ b	Secure and maintain any computer systems (network, hardware, and software applications) that will be used in the performance of this Agreement. This includes ensuring that all security patches, upgrades, and anti-virus updates are applied as appropriate to secure data that may be used, transmitted, or stored on such systems in the performance of this Agreement.	Yes	Updates and patches are checked for daily and applied daily on SCRE admin systems and Research VM Guest OSes. Host-based firewalls allow minimum communication required for operation of internal systems. No internet access permitted.
IV/ c	Store all the EDD's confidential documents in a physically secure manner at all times to prevent unauthorized access.	Yes	Project media stored in fire safe with combination lock inside of "High Security" area of North Hall Data Center (access controls via keycard, staffed 8 hours daily and alarmed)
IV/ d	Store the EDD's confidential electronic records in a secure central computer facility. Where in-use on a shared computer system or any shared data storage system, ensure appropriate information security protections are in place. UCSB shall ensure that appropriate security access controls, storage protections and use restrictions are in place to keep the confidential information in the strictest confidence and shall make the information available to its own personnel on a "need-to-know" basis only.	Yes	Access controls enabled on web VPN portal and within Research Virtual Desktop. Multi-factor authentication required.
IV/ e	Store the EDD's confidential data in encrypted format when recorded on removable electronic storage media, or on mobile computing devices, such as a laptop computer.	Yes	No removable storage media permitted.
IV/ f	Maintain an audit trail and record data access of authorized users and authorization level of access granted to the EDD's data, based on job function.	Yes	Logging enabled for all activity on web VPN portal, Research Virtual Desktop and File Transfer Gateway.
IV/ g	Direct all personnel permitted to use the EDD's data to avoid leaving the data displayed on their computer screens where unauthorized users may view it. Personnel should retrieve computer printouts as soon as they are generated so that the EDD's data is not left unattended in printers where unauthorized personnel may access them.	Yes	No printing is enabled/allowed from SCRE. 30 minute session timeouts in place for all web VPN sessions.
IV/ h	Dispose of confidential information obtained from the EDD, and any copies thereof made by UCSB, after the purpose for which the confidential information is disclosed is served. Disposal means	Yes	Secure-delete of Research Virtual Desktop VM images at end of project; secure disposal (shred) of original

RESTRICTED DATA PROVIDER REQUIREMENTS CROSSWALK

	return of the confidential information to the EDD or destruction of the information utilizing an approved method of confidential destruction, which includes electronic deletion (following Department of Defense specifications) shredding, burning, or certified or witnessed destruction.		project media
IV/ i	Comply with the California Unemployment Insurance Code (CUIC) on any matters pertaining to the access, use, and/or release of data under this agreement. Failure to comply with this provision shall be deemed a breach of this agreement and shall be grounds for cancellation of this Agreement.	Yes	
IV/ j	Instruct all UCSB staff with access to the information provided by the EDD under this Agreement regarding the: (1) the confidential nature of the information, if applicable; (2) the requirements of this Agreement; (3) the need to adhere to the security and confidentiality provisions outlined in Exhibit E – Protection of Confidentiality Provisions; and (4) the sanctions and penalties against unauthorized use or disclosure found in CUIC Sections 1094 and 2111, the California Civil Code Section 1798.55, and the California Penal Code Section 502.	Yes	
IV/ k	Ensure that all the UCSB staff assigned to work with the information provided by the EDD have signed the EDD Confidentiality Statement (Attachment E1. Rev 05/08/14).	Yes	
IV/ l	Comply with Title 20, Code of Federal Regulations Section 603.7 with respect to any of the EDD confidential information.	Yes	
IV/ m	Dispose of the EDD's confidential information using an approved method of confidential destruction.	Yes	Secure-delete of VM images at project completion, secure destruction of original project media
IV/ n	Not release the EDD's confidential information to any other public or private entity without the EDD's prior written consent.	Yes	
IV/ o	Cooperate with the EDD's authority to monitor this Agreement in accordance with Exhibit E, Section II, paragraphs (e) and (f).	Yes	