COUNTY OF LOS ANGELES
DOWNEY DATA CENTER
SECURID TOKEN RENEWAL REQUEST
For L.A. COUNTY EMPLOYEES

PROFILE INFORMATION – print or type			
DATE OF REQUEST	COUNTY EMPLOYEE #	EMAIL ADDRESS	TOKEN EXP. DATE
REQUESTOR NAME (LAST NAME, FIRST NAME MI)			WORK PHONE # ( )
COUNTY DEPARTMENT NAME/DIVISON/PROGRAM **MENTAL HEALTH**			COUNTY DEPT # **435**
WORK MAILING ADDRESS (Street, City, State, Zip)			
Check one ☐ TOKEN TO BE MAILED ☐ TOKEN TO BE PICKED UP			

SECURID REMOTE ACCESS – DMH APPLICATION COORDINATOR ONLY	
(ACCOUNT NUMBER is REQUIRED for processing.) BILLING ACCOUNT NUMBER _____	DEVICE TYPE: KEYFOB

☐ **VPN – check if you are a VPN customer.**

SECURITY STATEMENT FOR VPN CUSTOMERS

Before connecting to the County network you must install anti-virus software, and stay up-to-date with definitions, Microsoft patches (critical and security) and service packs. A Firewall, either hardware firewall or personal firewall software is required for those using broadband internet access (DSL, ISDN, cable modems, etc). You agree not to share your logon ID, password and SecurID passcode with others.

SIGNATURES – each signature entry must be completed in full.			
Your signature indicates that you have read and will comply with the above **SECURITY STATEMENT.** REQUESTOR'S SIGNATURE			
AUTHORIZED MANAGER/DESIGNEE SIGNATURE	PRINT NAME	PHONE ( )	DATE
COUNTY DMH DESIGNEE SIGNATURE	PRINT NAME **JOYCE FANTROY**	PHONE 213-351-1335	DATE

NOTE: If submitting a **PDF**, **FAX** or **COPY**, this section must be completed in order to process the request.

☐ **PDF** ☐ **FAX** ☐ **COPY**

AUTHORIZED MANAGER/DESIGNEE SIGNATURE	PRINT NAME	PHONE ( )	DATE

NAME (Print) **JOYCE FANTROY** **SIGNATURE:** _____

My signature above, stipulates that my department has setup a process to maintain the original form on file for a period of 7 years, and will make the original form available within 72 hours, upon request from ISD or those acting on the behalf of ISD, ie., internal or external Auditors.

WARNING: FAILURE TO FULLY COMPLETE & SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING.

MAIL FORM TO: COUNTY OF LOS ANGELES – DMH
CIOB/INFORMATION SECURITY – SYSTEMS ACCESS UNIT
695 S. VERMONT, 8TH FLOOR
LOS ANGELES, CA 90005

Revised 4/6/2010

COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE AND
CONFIDENTIALITY OF
COUNTY'S INFORMATION TECHNOLOGY ASSETS,
COMPUTERS, NETWORKS, SYSTEMS AND DATA

As a Los Angeles County employee, contractor, vendor or other authorized user of County Information Technology (IT) assets including computers, networks, systems and data, I understand that I occupy a position of trust. I will use County IT assets for County management approved business purposes only and maintain the confidentiality of County's business and Citizen's private data. As a user of County's IT assets, I agree to the following:

1. Computer crimes: I am aware of California Penal Code 502(c) - Comprehensive Computer Data Access and Fraud Act (attached). I will immediately report any suspected computer misuse or crimes to my Management.

2. Security access controls: I will not subvert or bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. I will not share my computer identification codes (log-in ID, computer access codes, account codes, ID's, etc.) or passwords.

3. Approved business purposes: I will use the County's Information Technology (IT) assets including computers, networks, systems and data for County management approved business purposes only.

4. Confidentiality: I will not access or disclose any County program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.

5. Computer virus and malicious code: I will not intentionally introduce any computer virus, worms or malicious code into any County computer, network, system or data. I will not disable or delete computer virus detection and eradication software on County computers, servers and other computing devices I am responsible for.

6. Offensive materials: I will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over County owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of my assigned job duties, e.g., law enforcement. I will report to my supervisor any offensive materials observed by me or sent to me on County systems.

7. Public Internet: I understand that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. I will use County Internet services for approved County business purposes only, e.g., as a research tool or for electronic communication. I understand that the County's Internet services may be filtered but in my use of them I may be exposed to offensive materials. I agree to hold the County harmless should I be inadvertently exposed to such offensive materials. I understand that my Internet activities may be logged, are a public record, and are subject to audit and review by authorized individuals.

8. Electronic mail and other electronic data: I understand that County electronic mail (e-mail), and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. I will comply with County e-mail use policy and use proper business etiquette when communicating over e-mail systems.

9. Copyrighted materials: I will not copy any licensed software or documentation except as permitted by the license agreement.

10. Disciplinary action for non-compliance: I understand that my non-compliance with any portion of this Agreement may result in disciplinary action including my suspension, discharge, denial of service, cancellation of contracts or both civil and criminal penalties.

CALIFORNIA PENAL CODE 502(c) - "COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT"

Below is a section of the "Comprehensive Computer Data Access and Fraud Act" as it pertains specifically to this Agreement. California Penal Code 502(c) is incorporated in its entirety into this Agreement by reference and all provisions of Penal Code 502(c) apply. For a complete copy, consult the Code directly at website www.leginfo.ca.gov/.

502.(c) Any person who commits any of the following acts is guilty of a public offense:

(1) Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongly control or obtain money, property, or data.

(2) Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

(3) Knowingly and without permission uses or causes to be used computer services.

(4) Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network.

(5) Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

(6) Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

(7) Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

(8) Knowingly introduces any computer contaminant into any computer, computer system, or computer network.

I HAVE READ AND UNDERSTAND THE ABOVE AGREEMENT:

Employee's Name	Employee's Signature	Date
Manager's Name	Manager's Signature	Date