COUNTY OF LOS ANGELES
MAINFRAME, UNIX, AND REMOTE ACCESS REGISTRATION FORM
For L.A. COUNTY EMPLOYEES and CONTRACTORS

PROFILE INFORMATION — Complete boxes 1 – 9

*Mandatory Fields

(1) *DATE OF REQUEST	(2) *TYPE OF REQUEST	(3) ☐ *EMPLOYEE OR ☑ CONTRACTOR #
	☐ NEW LOGON ID ☐ UPDATE LOGON ID ☐ DELETE LOGON ID	

(4) *LAST NAME , *FIRST NAME , MI	(5) E-MAIL ADDRESS

(6) *COUNTY DEPARTMENT NAME/ORGANIZATION NAME	(7) *COUNTY DEPARTMENT NUMBER
Los Angeles County Public Health Dept./Division of HIV and STD Programs (DHSP)	LAPH-DHSP/#296
(8) *WORK MAILING ADDRESS (STREET, CITY, STATE, ZIP)	**(9) *CELL PHONE NUMBER**
600 South Commonwealth Avenue, Los Angeles CA 90005	

IBM DATA CENTER ACCESS — Complete for required access, as defined by your management

(10) LOGON ID	(11) 2-DIGIT MAJOR GROUP CODE	(12) 2-DIGIT LSO GROUP CODE	(13) SECURITY AUTHORIZATION

☐ **TSO ACCESS — Check box for access and complete fields 10, 11, 12, and 13 (see above)**

(14) 2-DIGIT TSO GRP CODE	(15) BIN NUMBER	(16) SUG-GROUP 1	(17) SUB-GROUP 2	(18) SUB-GROUP 3

☐ **ONLINE ACCESS — Check box for access and complete fields 10, 11, 12, 13, 19, and 20**

(19) SYSTEM APPLICATION	(20) GRP NAME/NATURAL PROFILE	(21) OLD GRP/NATURAL PROFILE	DMV/JAI/APS APPLIATION COORDINATORS ONLY
			APS A/O:
			DMV SYSTEM CODE:
			JAI SYSTEM LOCATION:

UNIX ENVIRONMENT ACCESS — Complete for required access, as defined by your management

(22) TYPE OF REQUEST (Check One) ☐ ADD NEW LOGON ID ☐ UPDATE LOGON ID ☐ DELETE LOGON ID

(23) LOGON ID	(24) APPLICATION	(25) ACCESS GROUP

REMOTE ACCESS — Complete for required access (E-mail address required, see box #5)

☐ (26a) NEW TOKEN ☐ (26b) REPLACE LOST/STOLEN TOKEN ☐ (26c) REPLACE DEFECTIVE TOKEN ☐ (26d) RENEW TOKEN

Expiration Date:_____

PLEASE SELECT YOUR REMOTE ACCESS TYPE:

Note: When selecting an RSA SecurID Hard Token or Software Token, a valid Billing Account Number is **REQUIRED**

☑ **(27a) TOKENLESS AUTHENTICATION VPN**
Uses Password - Does Not Expire

☐ **(27b) HARD TOKEN SECURID VPN**
Uses Key Fob - 3 Year Expiration

☐ **(27c) SOFTWARE TOKEN SECURID VPN**
Uses Mobile Device or Computer - 3 Year Expiration

Select Device Type Below:

(28) BILLING ACCOUNT NUMBER for SecurID Token: _____

☐ IOS ☐ ANDROID ☐ COMPUTER

SECURITY STATEMENT: 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 a hardware firewall or personal firewall software, is required for those using broadband Internet access. You agree not to share your Logon ID, password, and SecurID passcode with others.

SIGNATURES — Please sign, enter phone number, print name, and date below

Your signature indicates that you have read and will comply with the above **Security Statement**.

(29) CUSTOMER'S SIGNATURE	(30) PHONE #	(31) NAME	(32) DATE
(33) MANAGER'S SIGNATURE	**(34) PHONE #**	**(35) MANAGER'S NAME**	**(36) DATE**
	(213) 639-4314	Waley Zeng	
(37) DEPARTMENT COORDINATOR'S SIGNATURE	**(38) PHONE #**	**(39) DEPARTMENT COORDINATOR'S NAME**	**(40) DATE**

WARNING: FAILURE TO FULLY COMPLETE & SIGN THIS FORM WILL CAUSE A DELAY IN PROCESSING.
You may submit completed registration forms to ISDRegistration@isd.lacounty.gov or the ISD Registration office at 9150 E. Imperial Hwy, Downey, CA 90242 Mail Stop # 29 to process.

For any questions related to registration please call (562) 940-3305.

Revised: April 2022

INSTRUCTIONS

COUNTY OF LOS ANGELES
MAINFRAME, UNIX, AND REMOTE ACCESS REGISTRATION FORM

For L.A. COUNTY EMPLOYEES and CONTRACTORS

PROFILE INFORMATION

1. **Mandatory**. Print or type the Date of the request
2. **Mandatory**. Check the appropriate type of request
3. **Mandatory.** Enter your six-digit County Employee or Contractor Number (if applicable)
4. **Mandatory.** Print your Last Name, First Name, and Middle Initial
5. **Mandatory.** Enter your Department or Organization's E-mail Address
6. **Mandatory.** Enter the full name of your County Department or Organization (e.g. Los Angeles Superior Court)
7. **Mandatory.** Enter your three-digit County Department Number
8. **Mandatory.** Enter your Business Street Address (include room or suite number if applicable)
9. **Mandatory.** Enter your working Cell Phone Number (this is required in order to enroll for MFA and reset your password)

IBM DATA CENTER ACCESS

10. **Mandatory.** Enter your existing Logon ID (If applicable)
11. **Mandatory.** Enter your two-digit department Major Group Code, as defined by your management
12. **Mandatory.** Enter your two-digit Local Security Group Code, as defined by your management
13. **Optional.** Complete if you have been designated as a Local Security Officer by your management

TSO ACCESS — Check box if this request applies to TSO Access

14. **Mandatory.** Enter the two-digit identifier of your TSO group, as defined by your management
15. **Optional.** Enter Downey BIN number
16. **Optional.** Enter the two-character identifier, as defined by your management
17. **Optional.** Enter the two-character identifier, as defined by your management
18. **Optional.** Enter the two-character identifier, as defined by your management

ONLINE ACCESS — Check box if this request applies to Online Access

19. **Mandatory.** Enter each CICS online or IMS system application you require access to, as defined by your management
20. **Mandatory.** Enter the Group Name for each system application you require access to, as defined by your management
21. **Mandatory.** Enter the Old Natural Group/Profile Name

UNIX ENVIRONMENT ACCESS — Check box if this request applies to UNIX Access

22. **Mandatory.** Check the appropriate type of request
23. **Mandatory.** Enter your existing Logon ID (if applicable)
24. **Mandatory.** Enter the application you require access to, as defined by your management
25. **Mandatory.** Enter your UNIX Access Group

REMOTE ACCESS

26a. **Mandatory.** Check box for a New token
26b. **Mandatory.** Check box to Replace a Lost/Stolen token
26c. **Mandatory.** Check box to Replace a Defective/Malfunctioned token
26d. **Mandatory.** Check box to Renew a token
27a. **Mandatory.** Check box for Tokenless Authentication (RSA Adaptive Authentication remote access to County-protected resources)
27b. **Mandatory.** Check box for an RSA SecurID Hardware token (Key Fob valid for 3 years)
27c. **Mandatory.** Check box for an RSA SecurID Software token (a file for your device) and indicate device type

iOS/Android - You will receive a QR Code or Hyperlink for your mobile device
Computer - You will receive a program (.stdid) file for your Windows/MacOS workstation
(You will need to install the RSA Software Token client)
Checking any of the boxes for #27 indicates your compliance with the following Security Statement:

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 a hardware firewall or personal firewall software, is required for those using broadband Internet access. You agree not to share your Logon ID, password, and SecurID passcode with others.

28. **Mandatory.** Enter a valid 11-digit Billing Account Number, as defined by your management

SIGNATURES (required)

29. – 32. **Mandatory.** Sign, enter phone number, print name of County Employee or Contractor, and date
33. – 36. **Mandatory.** Sign, enter phone number, print name of authorizing Manager, and date
37. – 40. **Mandatory.** Sign, enter phone number, print name of Department Application Coordinator, and date

If you have indicated a need to access a system not owned by your department, concurrence from the other department(s) is required.

COUNTY OF LOS ANGELES
AGREEMENT FOR ACCEPTABLE USE
AND CONFIDENTIALITY OF COUNTY INFORMATION ASSETS

All capitalized terms not defined in this agreement have the same meaning as set forth in Board of Supervisors Policy No. 6.100 - Information Security Policy.

As a County of Los Angeles (County) Workforce Member, and as outlined in Board of Supervisors Policy 6.101 "Use of County Information Assets," I understand and agree:

- That I occupy a position of trust, as such I will use County Information Assets in accordance with County and Departmental policies, standards, and procedures including, but not limited to, Board of Supervisors Policy 9.015 "County Policy of Equity" (CPOE) and Board of Supervisors Policy 9.040 "Investigations of Possible Criminal Activity Within County Government."
- That I am responsible for the security of information and systems to which I have access or to which I may otherwise obtain access even if such access is inadvertent or unintended. I shall maintain the confidentiality of County Information Assets (as defined in Board of Supervisors Policy 6.100 – Information Security Policy).

That County Information Assets must not be used for:

  - Any unlawful purpose.
  - Any purpose detrimental to the County or its interests.
  - In any way that undermines or interferes with access to or use of any County Information Asset for official County purposes.
  - In any way that hinders productivity, efficiency, customer service, or interferes with other County Workforce Members performance of his/her official job duties.
  - Personal purpose where activities are for private or personal gain or advantage (including financial gain), or an outside endeavor not related to County business. Personal purpose does not include incidental and Minimal Personal use of County Information Assets.
  - To falsely represent oneself, real or fictional, or send Information anonymously unless specifically authorized by Department management or to make an anonymous report through a proper reporting mechanism.
  - Any personal communication that I intend to keep confidential.

- That records, files, databases, and systems contain restricted, confidential or internal use information (i.e., Non-Public Information), as well as public information. I may access, read, or handle Non-Public Information to the extent required to perform my assigned duties. Although I may have access to Non-Public Information, I agree to not access such information unless it is necessary for the performance of my assigned duties. I understand that unauthorized access of Non-Public Information is beyond the scope of my employment.
- Not to divulge, publish, share, expose, or otherwise make known to unauthorized persons, organization, or the public any County Non-Public Information. I understand that:
  - I may divulge Non-Public Information to authorized County staff and managers, as necessary to perform my job duties.

- I may divulge Non-Public Information to others only if specifically authorized to do so by federal, state, or local statute, regulation or court order, and with the knowledge of my supervisor or manager and following proper County and Departmental procedures.
- I may not discuss Non-Public Information outside of the workplace or outside of my usual work area.
- I must consult my supervisor or manager on any questions I may have concerning whether particular information may be disclosed.

- To report any actual exposure of Information Security or a situation that could potentially result in an exposure, misuse, or crime relating to County Information Assets whether this is on my part or on the part of another person following proper County and Departmental procedures. I understand that I am expected to assist in protecting evidence of crimes relating to Information Assets and will follow the instructions of, and cooperate, with management and any investigative response team.
- I have no expectation of privacy or confidentiality concerning my activities related to the use of, or access to, County Information Assets, including anything I create, store, send, or receive using County Information Assets. My actions may be monitored, logged, stored, made public, and are subject to investigation, audit, and review without notice or consent.
- Not possess a County Information Asset without authorization. Although I may be granted authorization to possess and use a County Information Asset for the performance of my duties, I will never be granted any ownership, exclusive possession or property rights to County Information Assets. All Information Assets and Information is the property of the County. I must surrender County Information Assets upon request. Any Information Asset retained without authorization will be considered stolen and prosecuted as such.
- Not intentionally, or through negligence, damage or interfere with the operation of County Information Assets.
- To neither, prevent authorized access, nor enable unauthorized access to County Information Assets.
- To not make computer networks or systems available to others unless I have received specific authorization from the Information Owner.

  - Not share my computer identification codes and other authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric or multifactor tokens, and/or smartcards) with any other person or entity. Nor will I keep or maintain any unsecured record of my password(s) to access County Information Assets, whether on paper or electronic.
  - I am accountable for all activities undertaken through my authentication mechanisms (e.g., logon identification (ID), computer access codes, account codes, passwords, ID cards/tokens, biometric or multifactor tokens, and/or smartcards).
- To not intentionally introduce any malicious software (e.g., computer virus, spyware, worm, key logger, malicious code, or data), into any County Information Asset or any non-County Information Systems or networks.

- To not subvert or bypass any security measure or system which has been implemented to control or restrict access to County Information Assets and any restricted work areas and facilities.

    - Disable, modify, or delete computer security software (e.g., antivirus, antispyware, firewall, and/or host intrusion prevention software) on County Information Assets. I shall immediately report any indication that a County Information Asset is compromised following proper County and Departmental procedures.

- To not access, create, or distribute (e.g., via email, Instant Messaging or any other means) any offensive materials (e.g., text or images which are defamatory, sexually explicit, racial, harmful, or insensitive) on County Information Assets, unless authorized to do so as a part of my assigned job duties (e.g., law enforcement). I will report any offensive materials observed or received by me on County Information Assets following proper County and Departmental procedures.
- That the Internet is public and uncensored and contains many sites that may be considered offensive in both text and images. I shall use County Internet services in accordance with County and Departmental policies and procedures. I understand that County Internet services may be filtered and that my use of resources provided on the Internet may expose me to offensive materials. I agree to hold County harmless from and against any and all liability and expense should I be inadvertently exposed to such offensive material.
- That electronic communications (e.g., email, instant messages, etc.) created, sent, and/or stored using County electronic communications services are the property of the County. I will not distribute, forward or otherwise disseminate such electronic communications without valid business justification. I will use proper business etiquette when communicating using County electronic communications services.
- Only use County Information Assets to create, exchange, publish, distribute, or disclose in public forums and social media (e.g., blog postings, bulletin boards, chat rooms, Twitter, Instagram, Facebook, and other social media services) in accordance with County and Departmental policies, standards, and procedures.
- Not store County Non-Public Information on any Internet storage site except in accordance with County and Departmental policies, standards, and procedures.
- Not store County Non-Public Information on any removable storage devices except in accordance with County and Departmental policies, standards, and procedures
- Not copy or otherwise use any copyrighted or other proprietary County Information Assets (e.g., licensed software, documentation, and data), except as permitted by the applicable license agreement and approved by County Department management. Nor will I use County Information Assets to infringe on copyrighted material.
- Should I choose to use a personally owned endpoint or portable computing device to access, view, edit, and/or create County Non-Public Information:
    - I attest that the device meets County and Departmental requirements.
    - I understand that my personally owned Endpoint or Portable Computing Device may be subject to legal discovery or public disclosure to the extent that it was used as a repository for County Non-Public Information which was not stored in the appropriate County storage repository.

- Should I discover an Information Security Incident or a weakness in any Information Security control or that I have access to information or systems to which I should not, I will immediately report such information to my supervisor or IT service desk/support team. I will make myself available to the Information Security or Incident Response Teams during the resolution or investigation process.
- That noncompliance may result in disciplinary action (e.g., suspension, discharge, denial of access, and termination of contracts) as well as both civil and criminal penalties and that County may seek all possible legal redress.

I HAVE READ, UNDERSTAND AND ACCEPT THE ABOVE AGREEMENT:

Name	xxxxxx Employee Number	LAPH-DHSP/#296 Department
Signature	Date	